Kaseya 2

Standard Solution Package

Guia do usuário

Version 7.0

Português

October 8, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Capítulo 1

Introdução

Neste capítulo

Visão geral

O **Standard Solution Package** é um conjunto de objetos de dados, coletivamente denominado **conteúdo**, pré-carregado no VSA. A Kaseya definiu esse conteúdo para refletir soluções de práticas recomendadas para o gerenciamento de máquinas no ambiente de um cliente. O conteúdo, junto com a documentação e as metodologias, foi desenvolvido para ajudar administradores da Kaseya a aplicar, de forma rápida e consistente, um conjunto padrão de soluções de configuração recomendadas imediatamente após a implantação de agentes.

Recursos e capacidades

Os recursos e as capacidades envolvem melhorias na capacidade de uso do produto, Auditoria e inventário, Suporte remoto, Gerenciamento de correções, Monitoramento e alertas, Políticas, Automação, Relatórios e muito mais.

Módulos compatíveis

Este pacote foi desenvolvido com conteúdo e suporte para os principais módulos/recursos do Kaseya K2 (6.3), como Sistema, Agente, Auditoria, Controle remoto (incluindo LiveConnect), Gerenciamento de correções, Monitoramento, Procedimentos de agente, Centro de informações, Visualizações e Gerenciamento de políticas.

Software e plataformas de SO compatíveis

Plataformas de SO do agente compatíveis

Este pacote fornece conteúdo e suporte para as plataformas de SO a seguir em máquinas agentes.

- Microsoft Windows XP, 2003, 2003 R2, Vista, 2008, 2008 R2, 7, 2012
- Apple Macintosh Mac OS X 10.5 (Leopard), 10.6 (Snow Leopard), 10.7 (Lion), 10.8 (Mountain Lion)
- SuSE Linux Enterprise 10 e 11, Red Hat Enterprise Linux 5 e 6, Ubuntu 8.04 e versões posteriores, e OpenSuSE 11, CentOS 5 e 6

Sistemas de terceiros compatíveis

O ITSM-SS foi desenvolvido com conteúdo e suporte para os sistemas e aplicativos de 3º a seguir.

- E-mail/mensagens
  - Exchange 2003, 2007, 2010, SMTP, IMAP, POP3, Blackberry Enterprise Server
- Antivírus/Antimalware
  - Symantec AntiVirus v10, Corporate Edition 10, Endpoint Protection v11
  - McAfee VirusScan/Enterprise, Total Protection, Endpoint Protection
  - Sophos AntiVirus
  - Trend Micro OfficeScan v10, Worry-Free Business Security v11
  - AVG Technoligies AntiVirus v8
  - Kaspersky Endpoint Security v8
  - Microsoft Security Essentials, Forefront Endpoint Protection
  - Produtos de antivírus/antimalware de 3º integrados ao Microsoft Security Center
- Backup/Recuperação
  - Symantec Backup Exec v10/11/12/12.5/2010/2012
  - Computer Associates BrightStor ARCServe Backup r11.1/11.5/12/12.5/15

- Servidores de banco de dados
  - Microsoft SQL Server 2005/2008/2008 R2
- Acesso remoto
  - Terminal Server, Citrix MetaFrame/Presentation Server/XenApp
- Infraestrutura de rede
  - Microsoft Active Directory, Arquivo e impressão, Servidor DHCP, Servidor DNS, Servidor de FTP
- Servidores da Web
  - Microsoft IIS 6/7, SharePoint Server 2007/2010

Resumo do pacote

O **Standard Solution Package** de conteúdo é pré-carregado automaticamente no VSA. Alguns tipos de conteúdo são organizados por **gabinete Sistema** na árvore de objetos de dados. Estes incluem:

- **Políticas**: gerenciamento de políticas > Políticas
- **Procedimentos do agente**: procedimentos do agente > Criar/Agendar
- **Conjuntos de monitores** - Monitor > Conjuntos de monitores

Outros tipos de conteúdo são exibidos em listas suspensas exclusivas:

- **Visualizações**: uma lista de *visualizações* predefinidas com um prefixo `zz[SYS]` é exibida ao selecionar a lista supensa **Visualizar** na parte superior de qualquer página da máquina exibindo o filtro de ID de máquinas/ID de grupos.
- **Políticas de gerenciamento de correções**: uma lista predefinida de *políticas de aprovação e negação de gerenciamento de correções* com um prefixo `zz[SYS]` será exibida ao selecionar a lista suspensa **Gerenciamento de correções > Aprovação por política > Política**.
- **Conjuntos de eventos**: uma lista de *conjuntos de eventos* predefinidos com um prefixo `zz[SYS]` ao selecionar a lista suspensa **Monitor > Alertas do log de eventos > Definir eventos a serem correspondidos ou ignorados**.

Foco em serviços de TI

O **Standard Solution Package** foi desenvolvido para a realização de serviços comuns de TI geralmente fornecidos por um provedor de serviços de TI ou organização de suporte de TI. Esses serviços comuns de TI incluem:

Serviço de TI	Descrição
Configuração padrão	Fornece administração simplificada da configuração e do aprovisionamento de configurações básicas, bem como políticas de notificação de suporte remoto.
Auditoria/Inventário	Fornece dados de inventário de hardware/software atualizados para máquinas.
Gerenciamento de correção/atualização	Fornece recursos de gerenciamento de correções/atualização para aprimorar a estabilidade, reduzir vulnerabilidades e riscos associados a elas, bem como visibilidade em relação ao status de correções de máquinas.
Manutenção de rotina	Fornece manutenção de rotina para máquinas para mantê-las operacionais com mais eficiência.
Monitoramento	Fornece monitoramento contínuo de servidores e/ou estações de trabalho para serviços, dados de desempenho, processos, eventos, integridade e estabilidade em geral.
Relatório	Fornece recursos de geração de relatórios, que oferecem visibilidade sobre todos os aspectos dos vários serviços de suporte de TI sendo fornecidos.

Configuração automatizada e especializada do sistema

É fornecido conteúdo que é mais comumente aplicável a todas as máquinas que você gerencia. O restante do conteúdo predefinido representa um catálogo de soluções alternativas bem conhecidas que você deve considerar aplicar em circunstâncias especializadas.

- **Configuração automatizada do sistema**: conteúdo usado comumente que pode ser configurado de forma rápida e automática para uma organização específica usando o assistente de configuração **Systems Management Configuration**. Basta seguir as etapas na seção **Configuração de gerenciamento de sistemas** *(página 2)* deste guia. O conteúdo usado pelo assistente é descrito na seção **Conteúdo habilitado do assistente de configuração** *(página 15)* deste guia.
- **Configuração especializada do sistema**: depois que você executar o assistente de configuração **Systems Management Configuration**, poderá modificar as políticas aplicadas. Você também pode selecionar políticas ou conteúdo adicionais ou diferentes e reorganizar a configuração inicial para que se adapte aos requisitos de sua empresa. Essa capacidade de personalização é apresentada no tópico **Como personalizar as políticas de uma organização** *(página 10)*. A seção **Catálogo de conteúdo completo** *(página 59)* deste guia descreve os objetos de dados que estão disponíveis para uso.

Capítulo 2

Configuração de gerenciamento de sistemas

Neste capítulo

O assistente de configuração

A versão 6.3 do Kaseya **Virtual System Administrator™** apresenta o assistente de configuração **Systems Management Configuration**. O assistente de configuração permite *configurar e aplicar políticas de gerenciamento de máquinas para uma organização específica.* Uma vez configurado, essas políticas são atribuídas a todas as máquinas gerenciadas em nome da organização. As políticas regem vários aspectos diferentes de gerenciamento da máquina:

- Programação da auditoria
- Monitoramento
- Alertas
- Gerenciamento da correção
- Manutenção de rotina da máquina utilizando procedimentos do agente

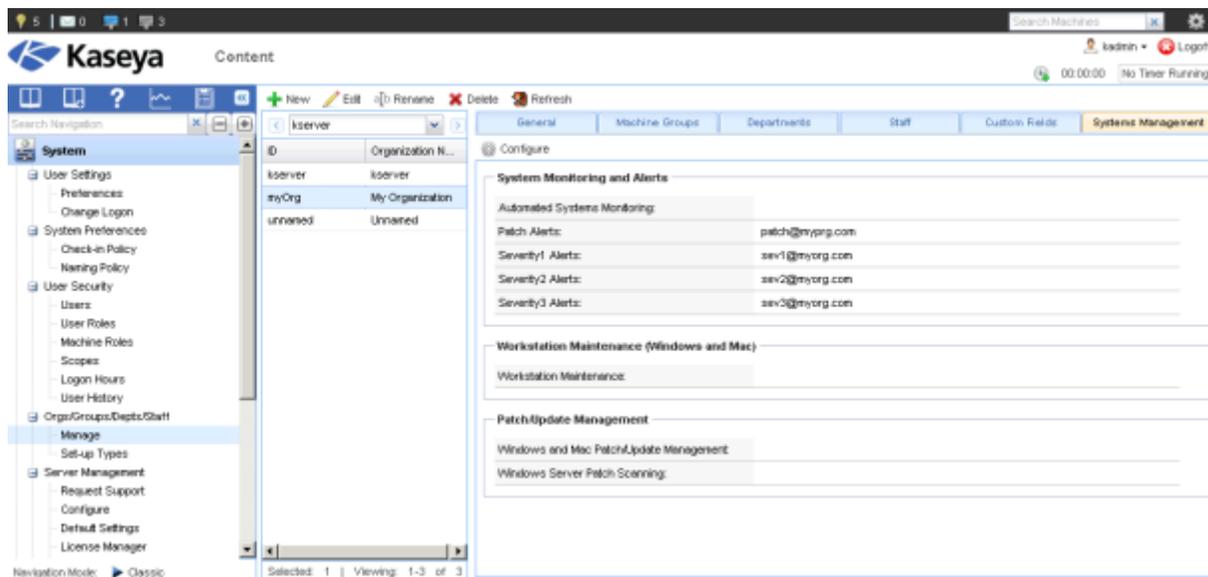
Com as políticas, não é mais necessário gerenciar cada máquina individualmente. Você só precisa atribuir ou alterar a política. A atribuição de políticas ou modificação de uma política atribuída é propagada no intervalo de 30 minutos para todas as máquinas participantes sem a necessidade de agendamento. Uma vez aplicadas, pode-se determinar rapidamente se máquinas gerenciadas estão em conformidade ou não com as políticas atribuídas. O acompanhamento da conformidade por política individual oferece as informações de que você necessita para oferecer serviços de TI de forma consistente em todas as organizações gerenciadas.

Observe o seguinte antes de executar o assistente de configuração **Systems Management Configuration** em qualquer organização.

- Você pode executar novamente o assistente de configuração **Systems Management Configuration** para selecionar diferentes opções para uma organização, desde que você não tenha atribuições de política personalizadas para a mesma organização no **Policy Management**.
- A execução do assistente de configuração **Systems Management Configuration** significa que você pretende gerenciar essa organização *por política*. Se você modificar *manualmente* a configuração do agente depois de aplicar uma política, haverá uma condição de "substituição de política". Por exemplo, fazer alterações no menu de agente de uma máquina usando a página **Menu do agente**, no módulo **Agente**, configura uma condição de substituição para essa máquina de agente. As políticas de substituição do **Policy Management** serão ignoradas a partir de então. A qualquer momento é possível apagar uma política de substituição usando o módulo **Policy Management**.

Como executar o assistente de configuração

1. Acesse a página **Sistema > Orgs/Grupo/Deptos/Equipe > Gerenciar**.
2. Selecione uma organização no painel central.
3. Selecione a guia **Gerenciamento de sistemas**.
4. Clique no botão **Configurar**.

Nota: Em um novo VSA sem agentes instalados ainda, você poderá ser solicitado pela barra de notificação a executar esse mesmo assistente de configuração para a organização `myOrg`.

Nesta seção

Página 1 do assistente de configuração - Alertas e monitoramento do sistema

- **Ativar monitoramento de sistemas automatizados**: quando o sistema detectar um item que pode ser acionado por alerta, ele criará um alarme e o notificará por e-mail.
- **Alertas de correção**: o endereço de e-mail exclusivo para notificações de e-mail de alerta de correção.

  Nota: Este endereço de e-mail não será usado, exceto se as caixas de seleção da **página do assistente Gerenciamento de correções** *(página 5)* forem marcadas.

- **Usar endereço de e-mail para todos os alertas**: desmarque esta caixa de seleção para ver três campos de *alerta de severidade* adicionais. Marque esta caixa de seleção para usar o mesmo endereço de e-mail inserido na caixa de edição de **Alertas de correção** para todos os quatro tipos de alertas.

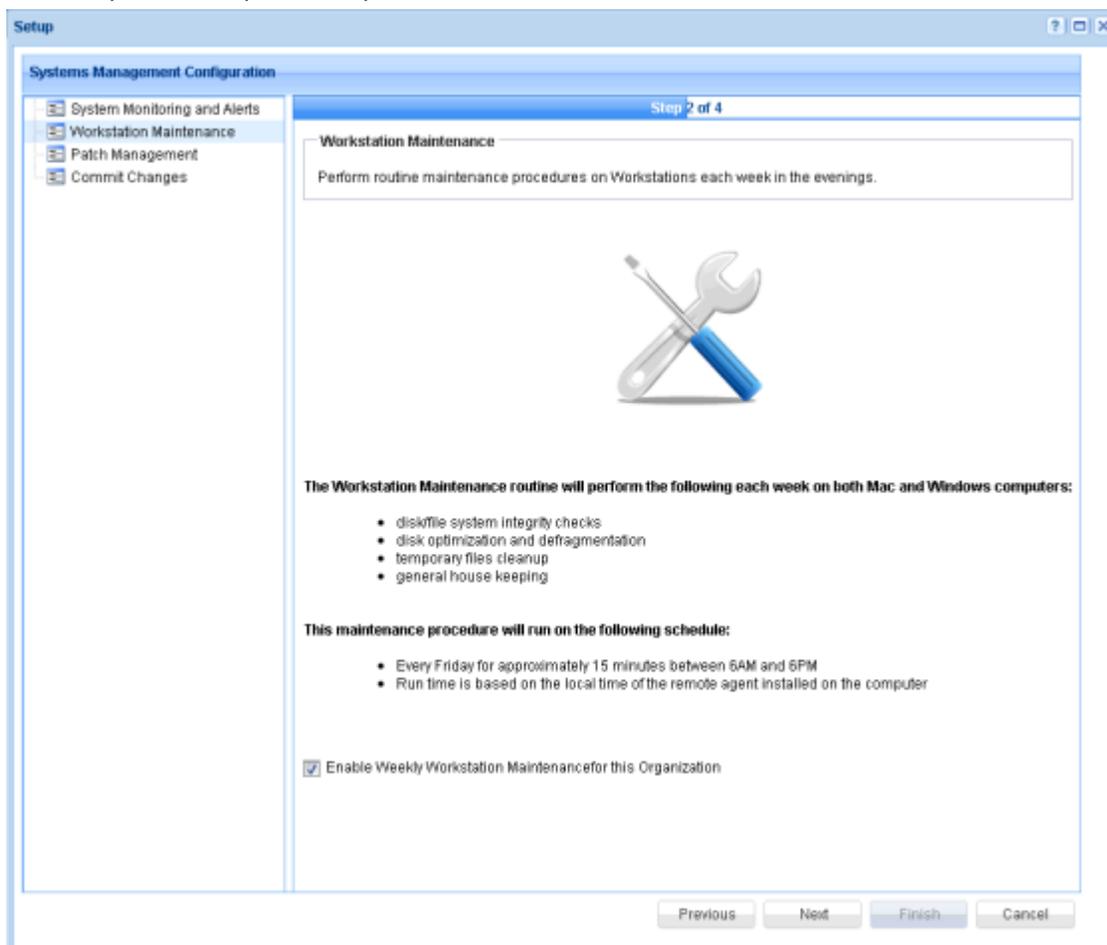
  Alertas de severidade se referem a todos os outros alertas, *exceto alertas de correção.* Diferentes tipos de alertas são considerados mais graves do que outros. Uma organização de TI pode ter várias equipes, cada uma respondendo a diferentes níveis de alertas.

  - **Alertas de severidade 1**: o endereço de e-mail para alertas de nível inferior.
  - **Alertas de severidade 2**: o endereço de e-mail para alertas de nível médio.
  - **Alertas de severidade 3**: o endereço de e-mail para alertas de nível superior.

Nota: Para permitir que várias organizações façam uso das mesmas políticas padrão incorporadas no **Policy Management**, **tokens** de espaço reservado são inseridos em campos de política exigindo um endereço de e-mail. Esses valores de token são `#patchAlertEmail#`, `#sev1AlertEmail#`, `#sev2AlertEmail#` e `#sev3AlertEmail#`. O VSA substitui automaticamente um valor de token em uma política pelo endereço de e-mail apropriado para uma organização específica quando uma condição de alerta é enviada. Os endereços de e-mail da organização que utilizam tokens são especificados usando esta página do assistente. As categorias de políticas do **Policy Management** que incluem endereços de e-mail são **Alertas**, **Conjuntos de monitores** e **Configurações de correções**.

Página 2 do assistente de configuração - Manutenção da estação de trabalho

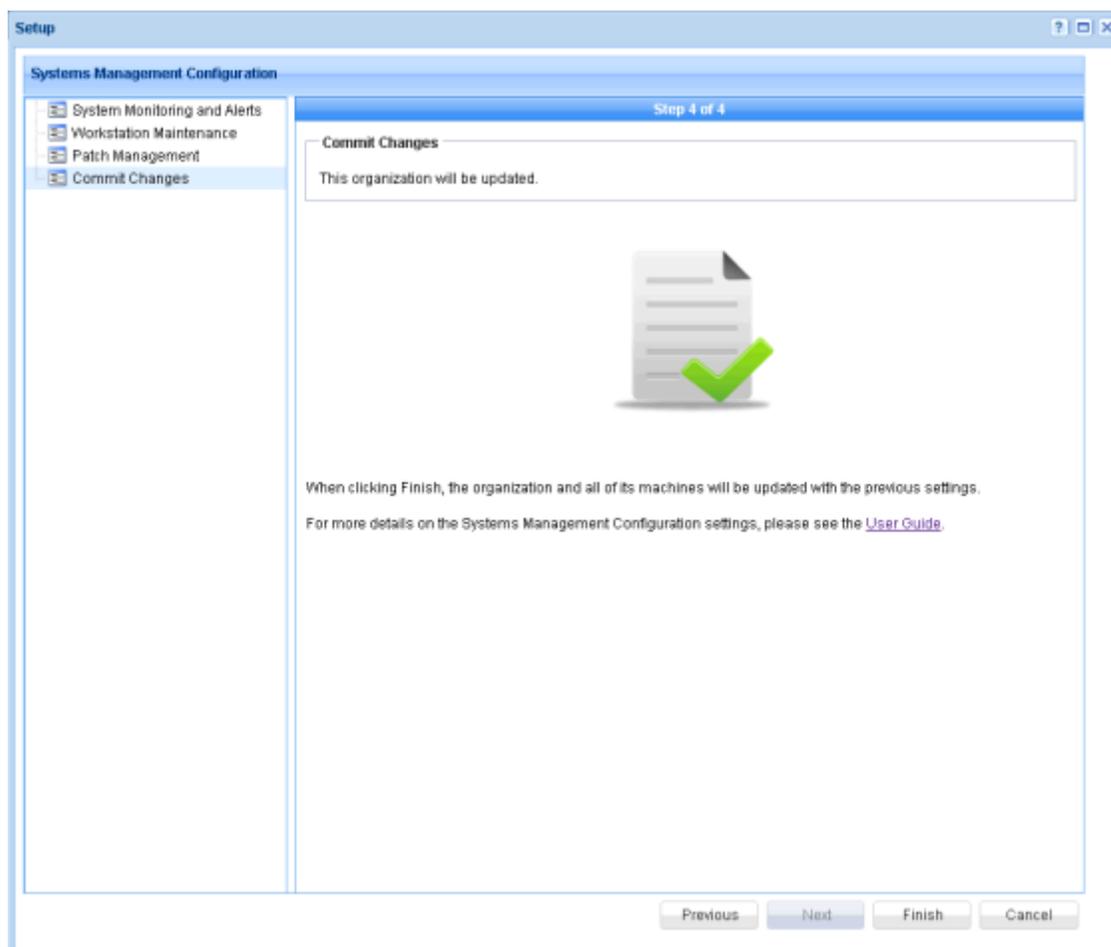
- **Ativar manutenção de estação de trabalho semanal**: se essa opção for marcada, as rotinas de manutenção semanal de estação de trabalho serão realizadas uma vez por semana, de segunda a sexta-feira, das 18h à 6h. Aplica-se somente a estações de trabalho com Windows e Macintosh. Não se aplica a Linux. Isso inclui o seguinte:

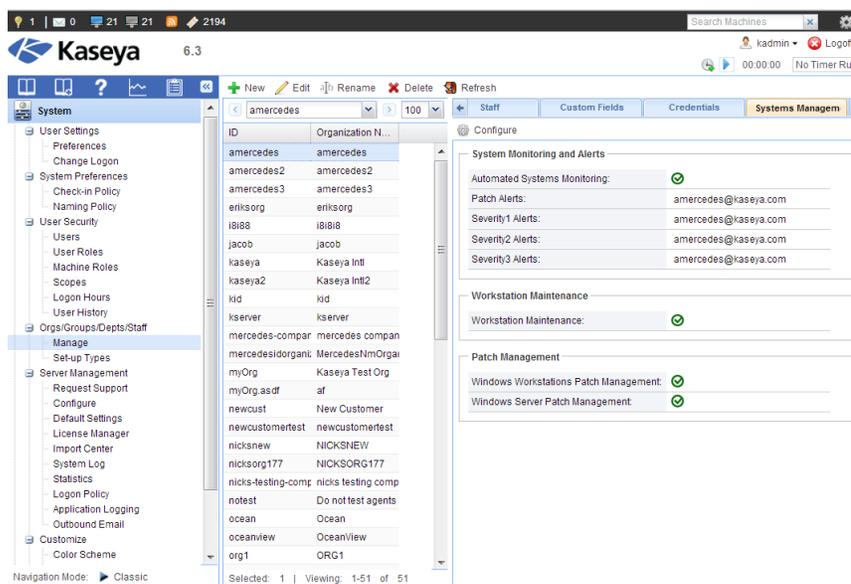
- ➢ Verificações de integridade do sistema de arquivos/disco
- ➢ Otimização e desfragmentação de disco
- ➢ Limpeza de arquivos temporários

Página 3 do assistente de configuração - Gerenciamento de correções

- **Ativar gerenciamento de correções e atualização da estação de trabalho**: se essa opção for marcada, todas as estações de trabalho com Windows serão verificadas e corrigidas automaticamente. Se uma correção exigir reinicialização, será enviada uma solicitação para o usuário a cada 60 minutos para que ele permita que a reinicialização seja feita.
- **Ativar verificação de correção do servidor com Windows**: todos os servidores com Windows serão automaticamente verificados quanto ao seu status atual. Nenhuma correção será instalada durante o processo. A verificação do servidor ocorrerá no período noturno. A correção de servidores deverá ser feita manualmente.
- **Credenciais do gerenciamento de correções**: o sistema criará automaticamente esta conta de administrador em cada computador. Isso afetará apenas computadores com agentes. É possível alterar ou excluir as credenciais a qualquer momento.

Nota: Uma credencial para essa nova conta é adicionada à página Auditoria > Gerenciar credenciais para esta organização. A nova credencial será designada como credencial de agente, o que significa que está configurada para atuar como a credencial de agente quando uma política ativada do **Systems Management Configuration** estiver em execução para essa organização.

Página 4 do assistente de configuração - Configuração concluída

Depois de clicar no botão **Concluir**, será exibida uma caixa de mensagem confirmando que a solicitação está sendo processada e levará até cinco minutos. As políticas para essa organização serão criadas e aplicadas a sistemas com agentes que pertencem a essa organização.

Confirmação na guia Gerenciamento do sistema

Quando o assistente de configuração **Systems Management Configuration** for encerrado, poderá levar até cinco minutos para que as políticas sejam aplicadas a máquinas gerenciadas na organização que você selecionou. Somente então você verá caixas de seleção em verde na guia **Gerenciamento do sistema**, confirmando que as opções que você escolheu usar foram aplicadas. As políticas aplicadas poderão, então, levar 30 minutos ou mais para serem propagadas para máquinas gerenciadas nessa organização.

Implementar agentes

Nesse ponto, a única tarefa restante a ser feita será adicionar máquinas gerenciadas a uma organização. Há várias formas para implantar agentes.

- **Discovery**: se você já tiver pelo menos um agente instalado em uma rede, o método recomendado para detectar e instalar agentes é usar o **módulo Discovery** *(http://help.kaseya.com/webhelp/PTB/KDIS/7000000/index.asp#7293.htm)*. A barra de notificação poderá pedir que você execute a detecção de rede quando uma nova rede for detectada.
- **Implementação de agente**: se você estiver implementando seu *primeiro* agente em uma nova rede, use então a página Agente > **Implementar agentes** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#491.htm)*. Para obter instruções sobre como instalar agentes, consulte o guia de início rápido para **implementação de agentes** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/PTB_agentdeployment70.pdf#zoom=70&navpanes=0)*.

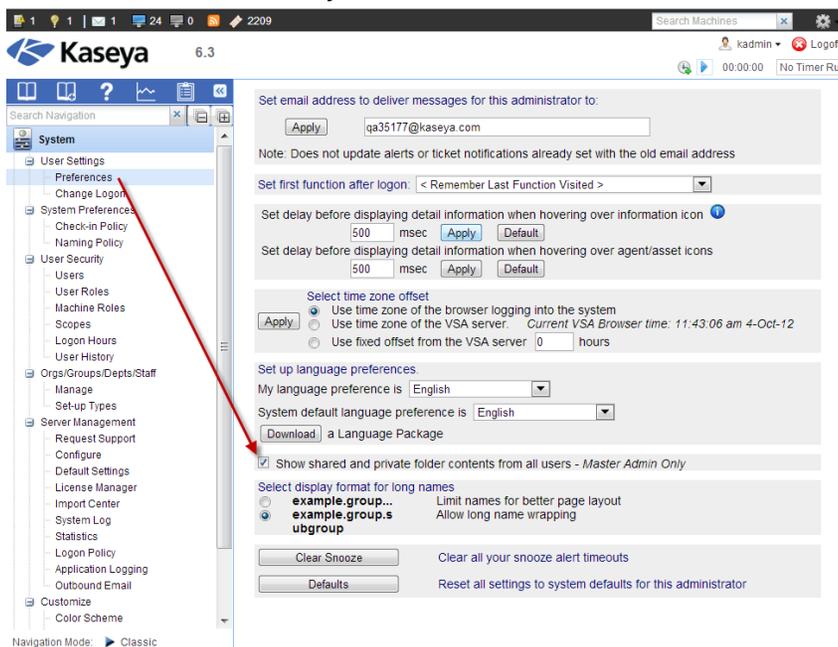
Lembre-se: o assistente de configuração **Systems Management Configuration** somente aplica políticas à organização que você acabou de selecionar. Certifique-se de que os agentes que você implementar sejam atribuídos a essa mesma organização.

Como funciona?

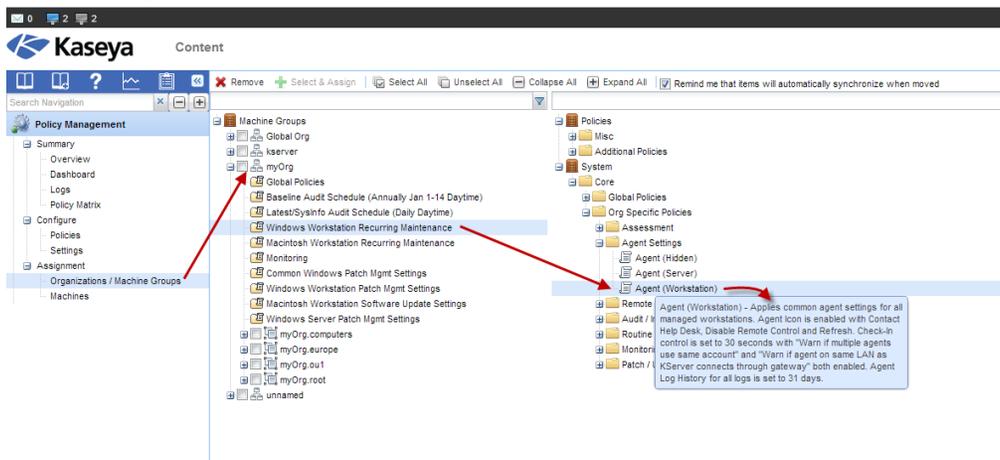
A seção **O assistente de configuração** *(página 2)* abordou apenas como usar o assistente de configuração **Systems Management Configuration**. Se isso é tudo o que você precisa saber, então poderá ignorar esta seção. Mas se você quer saber como o **Systems Management Configuration** utiliza a funcionalidade do VSA existente, continue lendo.

Nesta seção

Pré-requisitos

1. Certifique-se de que você esteja conectado ao VSA como *administrador mestre* em um VSA local ou como *administrador do sistema* em um VSA na nuvem. Isso garante que você terá acesso aos recursos discutidos nesta seção.
2. Certifique-se de que a caixa de seleção **Mostrar o conteúdo das pastas compartilhadas e privadas de todos os usuários - Somente o admin. mestre** esteja selecionada em **Sistema > Configurações do usuário > Preferências**. Essa caixa de seleção adicional fornece visibilidade das pastas do gabinete Sistema descritas nesta seção.

Políticas do sistema no gerenciamento de políticas

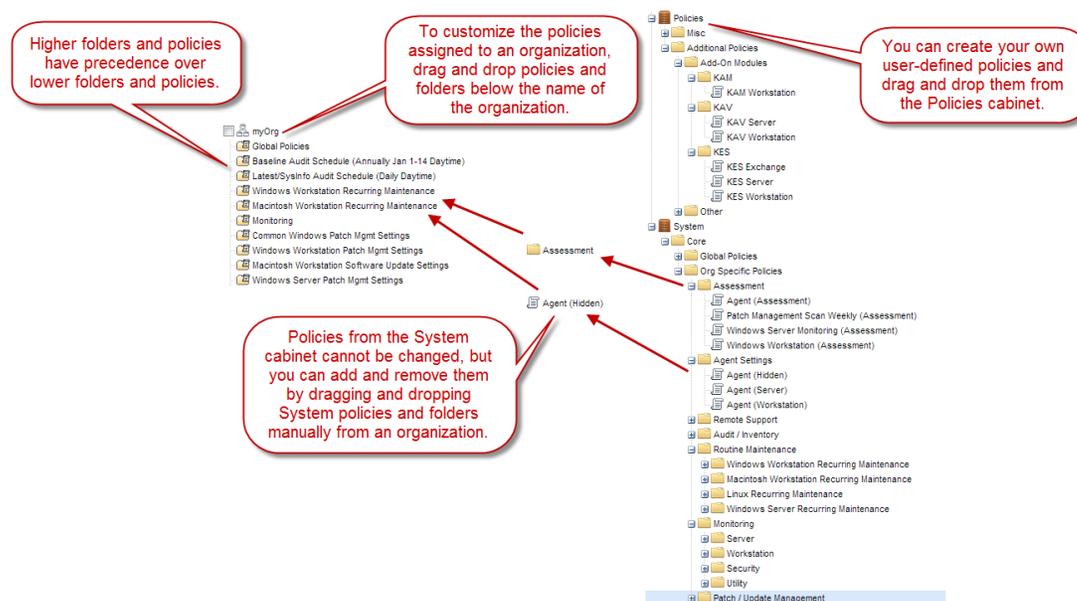
As escolhas feitas no assistente de configuração **Systems Management Configuration** criam uma lista de políticas que são aplicadas à organização que você selecionou. Vejamos essas políticas.

1. Acesse o módulo **Policy Management**.
2. Selecione a página **Organizações/Grupo de máquinas**.
3. Para a mesma organização que você selecionou ao executar o assistente de configuração **Systems Management Configuration**, expanda a pasta no painel central.
4. Expanda o gabinete **Sistemas** no painel direito.

Observe que qualquer pasta atribuída à sua organização tem uma pasta correspondente no painel direito. Essa pasta geralmente contém subpastas e conjuntos de políticas em cada subpasta. Passe o cursor sobre qualquer política específica para ver a descrição dessa política predefinida. Cada máquina gerenciada na organização selecionada será agora gerenciada por esta política, junto com todas as outras políticas atribuídas a essa organização.

Como personalizar as políticas de uma organização

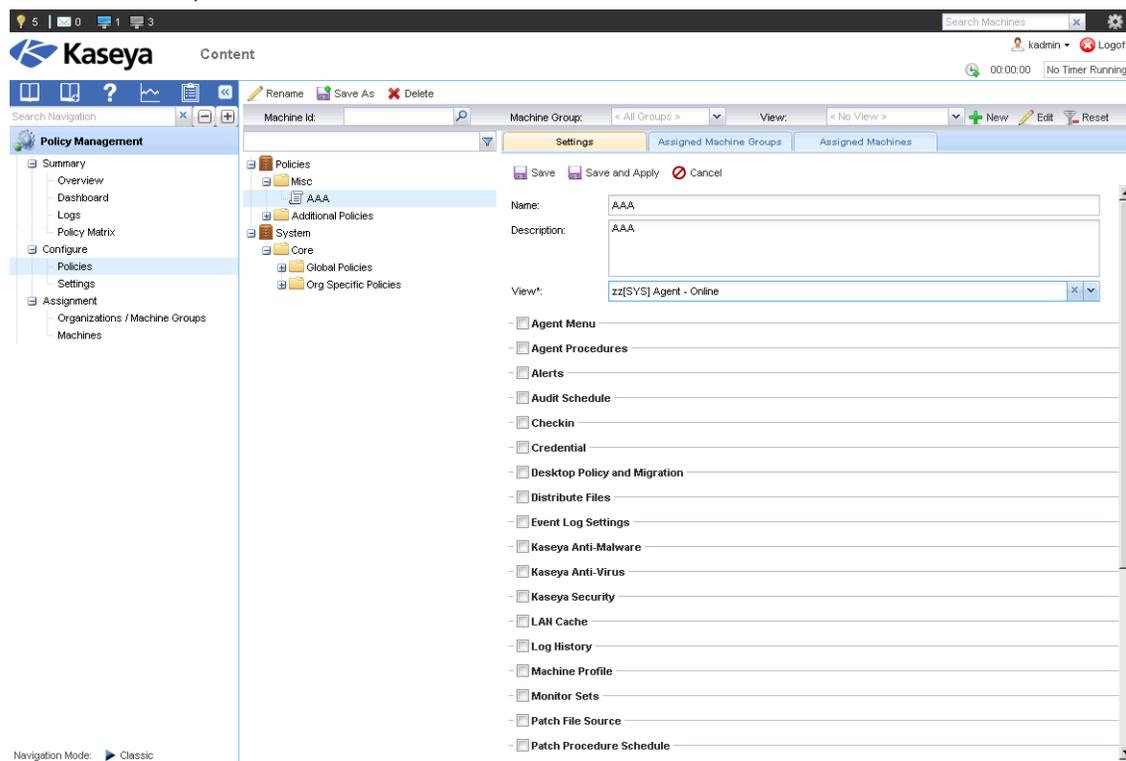
Mesmo sem saber em detalhes como as políticas são configuradas, você pode começar a personalizar as políticas que são atribuídas a uma organização específica.

Usando a página **Policy Management > Organizações/Grupo de máquinas**, você pode personalizar as políticas atribuídas a uma organização arrastando e soltando manualmente pastas ou políticas para a árvore da organização e desde dela. Isso inclui remover políticas do gabinete Sistema de uma organização, se desejar. Observe que **regras de atribuição de política** *(http://help.kaseya.com/webhelp/PTB/KPM/7000000/index.asp#8140.htm)* aplicam-se ao sequenciamento de políticas relacionadas abaixo de uma organização.

Políticas e pastas adicionais podem ser arrastadas e soltas do gabinete Sistemas ou do gabinete Políticas. As políticas do gabinete Sistema não podem ser modificadas, mas há mais políticas do gabinete Sistema disponíveis do que as que podem ser selecionadas usando o assistente de configuração **Systems Management Configuration**. Antes de tentar criar suas próprias políticas definidas pelo usuário, certifique-se de analisar as políticas do gabinete Sistema disponíveis. O conjunto completo de políticas do gabinete Sistema é descrito na seção **Conteúdo habilitado do assistente de configuração** *(página 15)* deste documento. Se você quiser saber mais sobre como uma política é criada, consulte o tópico **Detalhes da política** *(página 11)*.

Detalhes da política

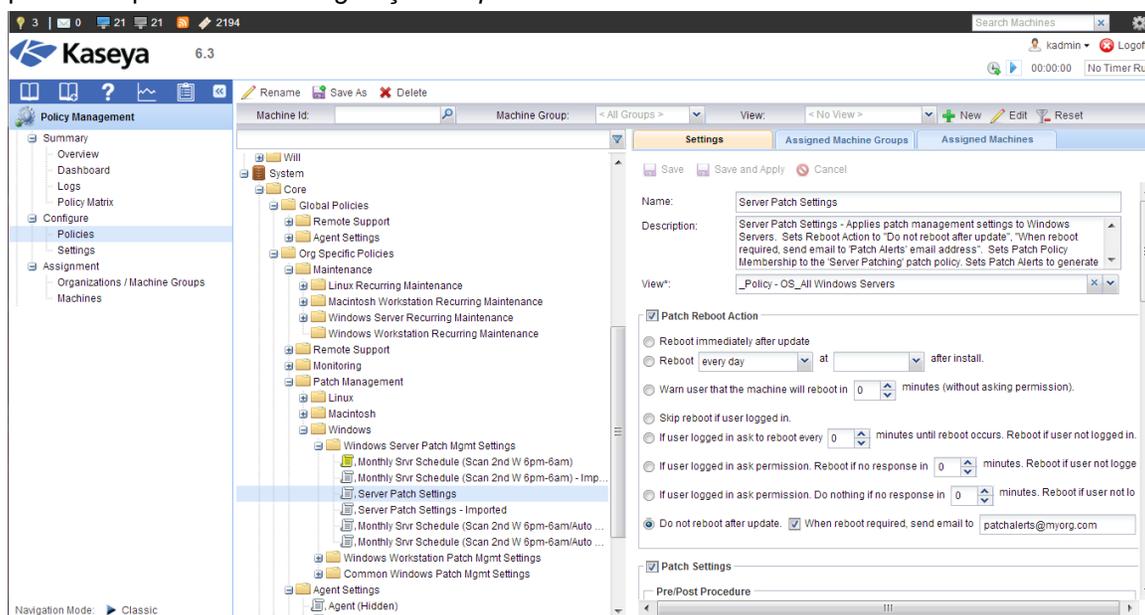
> **Nota:** Os próximos três tópicos descrevem resumidamente como uma política é criada. Para obter mais informações sobre políticas, consulte a **ajuda on-line e o guia de usuário do** *(http://help.kaseya.com/webhelp/PTB/KPM/7000000/index.asp#8410.htm)* **Policy Management**.

Os detalhes de cada política, seja uma política do Sistema ou uma política definida pelo usuário, podem ser inspecionados usando a página **Políticas**. Uma nova política pode opcionalmente incluir muitas categorias de configuração diferentes. Por exemplo, uma única política poderia definir propriedades de entrada do agente, definir um agendamento de auditoria e executar procedimentos do agente, tudo ao mesmo tempo.

A imagem a seguir mostra uma lista parcial de categorias de configuração disponíveis para uso ao criar uma nova política.

Configurações integradas versus configurações específicas de dados

Quando você analisar ou definir configurações de política em uma política específica, você observará dois tipos de configurações:

- **Configurações integradas**: essas configurações de política geralmente são caixas de seleção ou opções. Elas atribuirão a configuração a uma máquina gerenciada e isso é tudo o que você precisará especificar na política.
- **Configurações específicas de dados**: essas configurações de política especificam um *objeto de dados que já existe em outra parte no VSA*. Independentemente de esse objeto de dados fazer parte do conteúdo padrão que foi pré-carregado no VSA ou se é um objeto de dados que outro usuário do VSA criou e está usando com a política.

Por exemplo, na imagem a seguir, uma política de Sistema predefinida mostra a política de "reinicialização" de uma máquina depois que as atualizações de correção foram aplicadas. Essa é uma *configuração integrada* que não requer que você especifique qualquer outro objeto de dados. O próximo tópico aborda *configurações específicas de dados*.

Como vincular políticas a objetos de dados

Definir uma configuração específica de dados em uma política requer a especificação de um objeto de dados em outra parte do VSA.

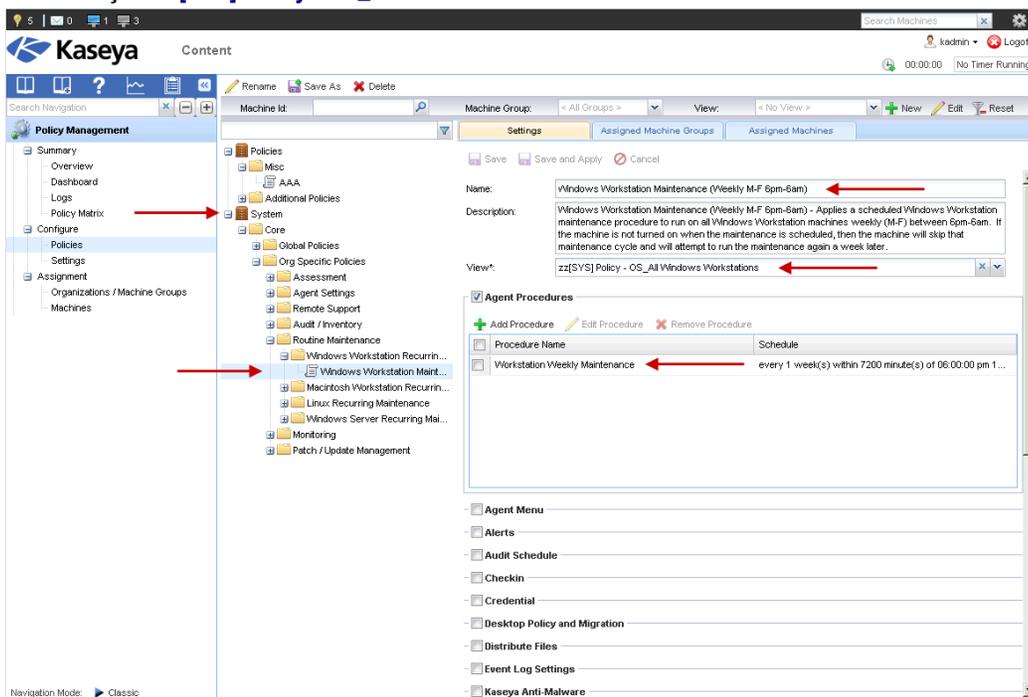
Lembre-se de que as políticas do gabinete Sistema no **Policy Management** são apenas um tipo de *conteúdo padrão* que é pré-carregado no VSA. Outros tipos de conteúdo incluem:

- Vistas
- Políticas de correção
- Conjunto de eventos
- Conjuntos de monitores
- Procedimentos do agente

Muitas das soluções automatizadas fornecidas pelo assistente de configuração **Systems Management Configuration** são ativadas vinculando-se políticas predefinidas do Sistema a esses outros tipos de objetos de dados predefinidos do Sistema.

Por exemplo, na imagem a seguir, vemos os detalhes de uma política do gabinete Sistema intitulada **Manutenção de estação de trabalho com Windows (semanal, de segunda a sexta, das 18h às 6h)**.

- Essa política agenda a execução semanal de um procedimento do agente intitulado **Manutenção semanal de estação de trabalho**.

- Observe também que essa mesma política está restrita a máquinas que pertencem à visualização **zz[SYS] Policy - OS_All Windows Workstations**.

Esse é apenas um exemplo de como as políticas do Sistema são vinculadas ao conteúdo do Sistema em qualquer outra parte no VSA. Use esse mesmo método para examinar as configurações e os links de qualquer outra política. Exceto para o fato de que não é possível modificar conteúdo e políticas do Sistema, lembre-se de que não há nada exclusivo sobre como eles são configurados. Quando você estiver pronto para tentar sozinho, crie seu próprio conteúdo e políticas definidas pelo usuário e os vincule juntos como você vê aqui. Se desejar, você pode fazer uma cópia de uma política do Sistema usando o botão **Salvar como** e começar sua personalização a partir daqui.

> **Nota:** Para obter mais informações sobre políticas, consulte a **ajuda on-line e o guia de usuário** *(http://help.kaseya.com/webhelp/PTB/KPM/7000000/index.asp#8410.htm)* do **Policy Management**.

Capítulo 3

Conteúdo habilitado do assistente de configuração

Os tópicos a seguir resumem as capacidades de conteúdo desenvolvidas para uso com o assistente de configuração **Systems Management Configuration**. Esse mesmo conteúdo pode ser usado manualmente sem o assistente.

Neste capítulo

Configuração padrão

Objetivo

Fornece administração simplificada da configuração e do aprovisionamento de configurações básicas, bem como políticas de notificação de suporte remoto.

Visão geral

Os agentes Kaseya têm uma variedade de definições de configuração que devem ser gerenciadas consistentemente em todas as máquinas gerenciadas, como Menu do agente, Controle de entrada, Diretório de trabalho, Definir credencial, Histórico do log, Configurações do log de eventos e Políticas de notificação de controle remoto. A Configuração de agentes padrão atende à necessidade de gerenciamento consistente em todos os sistemas para essas definições de configuração básicas que abrangem todo o sistema.

Políticas

Um conjunto de políticas é fornecido e é aplicável a definições de configuração do agente padrão em todas as máquinas na infraestrutura de TI compatível. Essas políticas controlam essas configurações como o Menu do agente, Controle de entrada, Diretório de trabalho, Definir credencial, Histórico do log, Configurações do registro de eventos e Políticas de notificação de controle remoto com base em um caso de uso de configuração do sistema de práticas recomendadas para operações em geral. As políticas estão localizadas em **[System].Core.Global Policies** e são descritas a seguir.

- **Configurações do agente**
  - **Agent (Core)**:aplica configurações comuns do agente para todas as máquinas gerenciadas. O ícone de agente está ativo, somente a opção Atualizar está ativada. O controle de entrada está definido como 30 segundos com as opções "Avisar se houver vários agentes usando a mesma conta" e "Avisar se o agente na mesma LAN que o KServer se conectar através do gateway" ativadas. O histórico de logs do agente para todos os logs está definido como 31 dias.
  - **Agente Windows**: aplica configurações do agente específicas para Windows. Define o diretório de trabalho do agente como c:\kworking.
  - **Agente Linux**: aplica configurações do agente específicas para Linux. Define o diretório de trabalho do agente como /tmp/kworking.
  - **Agente Macintosh**: aplica configurações do agente específicas para Macintosh Workstations. Define o diretório de trabalho do agente como /Library/kworking.
- **Suporte remoto**
  - **Política de notificação de CR de servidor (silencioso com ação de admin.)**: aplica a configuração de notificação de CR a todos os servidores. Define o tipo de notificação de usuário como Assumir controle silenciosamente; além disso, ativa a opção Requer a ação do admin para iniciar o controle remoto.
  - **Política de notificação de CR de estação de trabalho (alerta/termo com ação de admin.)**: aplica configurações de notificação de CR a todas as estações de trabalho. Define o tipo de notificação de usuário como Se o usuário estiver conectado exibir um alerta, Notificar o usuário quando a sessão terminar e ativa a opção Requer a ação do admin. para iniciar o controle remoto.

Auditoria/Inventário

Objetivo

Fornece uma estratégia de auditoria/inventário de rotina para suporte à visibilidade de ativos de hardware e software para planejamento a longo prazo, conformidade, projetos a curto e longo prazo, suporte a decisões e solução de problemas.

Visão geral

O Kaseya é compatível com vários tipos de auditorias de agente para detectar hardware e software implementados em uma infraestrutura de TI. Essas podem ser divididas em auditorias mais recentes, de linha de base e de informações do sistema. As auditorias mais recentes atualizam gradualmente informações atuais de hardware e software sobre máquinas. As auditorias de linha de base fornecem uma imagem em um ponto do tempo das informações de hardware e software sobre máquinas. As auditorias de informações do sistema fornecem detalhes adicionais sobre hardware usando SMBIOS. Para manter informações disponíveis sobre máquinas atualizadas para que decisões estratégicas e táticas possam ser tomadas, é importante agendar essas auditorias para que sejam executadas em algum padrão recorrente regularmente. Com essas informações de auditoria deve haver formas fáceis de localizar tipos específicos de sistemas com base nos dados de inventário detalhados conhecidos sobre eles, bem como deve haver formas de gerar relatórios e atuar com eficácia em relação a esses grupos de máquinas, se necessário.

Políticas

Um conjunto de políticas é fornecido e é aplicável a auditorias recorrentes a serem agendas em todas as máquinas na infraestrutura de TI compatível. Essas políticas permitem a coleta de informações críticas para o caso de uso de serviço de auditoria/inventário. As políticas estão localizadas em **[System].Core.Org Specific Policies.Audit / Inventory** e são descritas a seguir.

- **Baseline.Baseline Audit Schedule (Annually Jan 1-14 Daytime)**
  - **Agendamento de auditoria da linha de base (anualmente, de 1º a 14 de janeiro, das 6h às 18h/gestão de energia)**: aplica uma auditoria de linha de base anual agendada para todas as máquinas que foram implantadas e iniciadas, de 1º de janeiro a 14 de janeiro, entre 6h e 18h. A política usa o recurso de gestão de energia no horário de auditoria agendado, tentando ativar uma máquina desligada antes da auditoria. A política é geralmente usada em situações em que auditorias anuais podem ser necessárias para fins de planejamento ou conformidade; comparações de auditoria de linha de base/mais recentes relevantes também podem ser realizadas para tarefas operacionais. A política pode ser seletivamente aplicada a várias máquinas, grupos de máquinas e/ou organizações inteiras de máquinas.
- **Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Daytime)**
  - **Agendamento de auditoria mais recente/SysInfo (diariamente, de segunda a sexta, das 6h às 18h/gestão de energia)**: aplica auditorias de informações do sistema e mais recentes agendadas a todas as máquinas que entraram em execução diariamente (de segunda a sexta), das 6h às 18h. A política usa o recurso de gestão de energia no horário de auditoria agendado, tentando ativar uma máquina desligada antes da auditoria. Em geral, a política é usada em situações nas quais clientes precisam realizar auditorias durante o horário comercial em dias de semana, pois as máquinas geralmente estão desligadas à noite e em finais de semana. A política pode ser seletivamente aplicada a várias máquinas, grupos de máquinas e/ou organizações inteiras de máquinas.

Vistas

Um conjunto de visualizações predefinido é fornecido e pode ser usado em todos os aspectos do gerenciamento de serviços de TI, bem como para suporte ao serviço de auditoria/inventário. Essas visualizações fornecem a capacidade de filtrar máquinas no sistema com base em seu hardware, software e sua função. As visualizações a seguir podem ser usadas em atividades de geração de relatórios e operacionais.

Visualizar nome	Descrição
zz[SYS] HW - Dell	Exibe todas as máquinas com Dell como fabricante.
zz[SYS] HW - Dell PowerEdge	Exibe todas as máquinas com Dell como fabricante e PowerEdge no nome do produto.
zz[SYS] HW - HP	Exibe todas as máquinas com HP ou Hewlett Packard como fabricante.
zz[SYS] HW - HP ProLiant	Exibe todas as máquinas com HP ou Hewlett Packard como fabricante e ProLiant no nome do produto.
zz[SYS] HW - IBM	Exibe todas as máquinas com IBM como fabricante.
zz[SYS] HW - IBM Series X	Exibe todas as máquinas com IBM como fabricante e Series X no nome do produto.
zz[SYS] HW - Lenovo	Exibe todas as máquinas com Lenovo como fabricante.
zz[SYS] HW - Not Portable	Exibe todas as máquinas que não são móveis.
zz[SYS] HW - Portable	Exibe todas as máquinas que são móveis (ou seja, tipo de chassi = notebook ou laptop; portátil ou tablet pc; portátil ou subnotebook, ou netbook).
zz[SYS] HW - Under 1GB Memory	Exibe todas as máquinas que tenham menos de 1 GB de memória.
zz[SYS] HW - Under 512MB Memory	Exibe todas as máquinas que tenham menos de 512 MB de memória.
zz[SYS] HW - Virtual Guest	Exibe todas as máquinas que são computadores virtualizados (guests VMware, XenServer, VirtualBox ou HyperV).
zz[SYS] Network - 10.11.12.x	Exibe agentes de rede 10.11.12.x específica.
zz[SYS] OS - All Linux	Exibe todas as máquinas Linux.
zz[SYS] OS - All Mac OS X	Exibe todas as máquinas Mac OS X.
zz[SYS] OS - All Mac OS X Servers	Exibe todas as máquinas Mac OS X Server.
zz[SYS] OS - All Mac OS X Workstations	Exibe todas as máquinas Mac OS X Workstation.
zz[SYS] OS - All Servers	Exibe todas as máquinas executando um sistema operacional de classe de servidor.
zz[SYS] OS - All Windows	Exibe todas as máquinas com Windows.
zz[SYS] OS - All Windows SBS	Exibe todas as máquinas com Windows SBS Server.
zz[SYS] OS - All Windows Servers	Exibe todas as máquinas com Windows Server.
zz[SYS] OS - All Windows Workstations	Exibe todas as máquinas com Windows Workstation.
zz[SYS] OS - All Workstations	Exibe todas as máquinas executando um sistema operacional de classe de estação de trabalho.
zz[SYS] OS - Mac OS X 10.5 Leopard	Exibe todas as máquinas com Mac OS X 10.5.
zz[SYS] OS - Mac OS X 10.6 Snow Leopard	Exibe todas as máquinas com Mac OS X 10.6.
zz[SYS] OS - Mac OS X 10.7 Lion	Exibe todas as máquinas com Mac OS X 10.7.
zz[SYS] OS - Mac OS X 10.8 Mountain Lion	Exibe todas as máquinas com Mac OS X 10.8.
zz[SYS] OS - Win 2003 SBS	Exibe todas as máquinas executando um sistema operacional Windows 2003 Small Business Server.
zz[SYS] OS - Win 2003 Server	Exibe todas as máquinas executando um sistema operacional Windows 2003 Server.
zz[SYS] OS - Win 2008 R2 Server	Exibe todas as máquinas executando um sistema operacional Windows 2008 Server R2.
zz[SYS] OS - Win 2008 SBS	Exibe todas as máquinas executando um sistema operacional Windows 2008 Small Business Server.
zz[SYS] OS - Win 2008 Server	Exibe todas as máquinas executando um sistema operacional

	Windows 2008 Server.
zz[SYS] OS - Win 2012 Server	Exibe todas as máquinas executando um sistema operacional Windows 2012 Server.
zz[SYS] OS - Win 7	Exibe todas as máquinas executando um sistema operacional Windows 7.
zz[SYS] OS - Win Vista	Exibe todas as máquinas executando um sistema operacional Windows Vista.
zz[SYS] OS - Win XP	Exibe todas as máquinas executando um sistema operacional Windows XP.
zz[SYS] Role - BackupExec Server	Exibe todos os servidores BackupExec.
zz[SYS] Role - Blackberry Server	Exibe todos os servidores Blackberry Enterprise.
zz[SYS] Role - BrightStor ARCserve Server	Exibe todos os servidores BrightStor ARCserve.
zz[SYS] Role - Citrix Server	Exibe todos os servidores Citrix.
zz[SYS] Role - DHCP Server	Exibe todos os servidores MS DHCP.
zz[SYS] Role - DNS Server	Exibe todos os servidores MS DNS.
zz[SYS] Role - Domain Controller	Exibe todos os servidores MS AD Domain Controller.
zz[SYS] Role - Exchange 2003 Server	Exibe todos os servidores MS Exchange 2003.
zz[SYS] Role - Exchange 2007 Server	Exibe todos os servidores MS Exchange 2007.
zz[SYS] Role - Exchange 2010 Server	Exibe todos os servidores MS Exchange 2010.
zz[SYS] Role - Exchange Server	Exibe todos os servidores MS Exchange.
zz[SYS] Role - File Server	Exibe todos os servidores MS File com compartilhamentos de arquivos não admin.
zz[SYS] Role - FTP Server	Exibe todos os servidores MS FTP.
zz[SYS] Role - IIS Server	Exibe todos os servidores MS IIS.
zz[SYS] Role - IMAP4 Server	Exibe todos os servidores MS IMAP4.
zz[SYS] Role - POP3 Server	Exibe todos os servidores MS POP3.
zz[SYS] Role - Print Server	Exibe todos os servidores MS Print com compartilhamentos de arquivos não admin.
zz[SYS] Role - SharePoint Server	Exibe todos os servidores MS SharePoint.
zz[SYS] Role - SMTP Server	Exibe todos os servidores MS SMTP que também não são servidores MS Exchange.
zz[SYS] Role - SQL Server	Exibe todos os servidores MS SQL.
zz[SYS] Role - SQL Server (Default Instance)	Exibe a configuração de todos os servidores MS SQL com a instância padrão.
zz[SYS] Role - SQL Server 2005	Exibe todos os servidores MS SQL 2005.
zz[SYS] Role - SQL Server 2008	Exibe todos os servidores MS SQL 2008.
zz[SYS] Role - Terminal Server	Exibe todos os servidores MS Terminal em Modo aplicativo.
zz[SYS] Role - WINS Server	Exibe todos os servidores MS WINS.

Gerenciamento de correção/atualização

Objetivo

Fornecer uma estratégia de gerenciamento de correções/atualizações de rotina de máquinas gerenciadas para incluir varredura e corrreções, políticas de aprovação de correções, controle de comportamento de correções e visibilidade de status/conformidade de correções para suporte a

decisões e solução de problemas.

Visão geral

O Kaseya Patch Management é compatível apenas com correções do Microsoft Windows. Um status de correção de máquinas é detectado através de uma Varredura de correções; a implementação de correções é realizada através de agendamento de Atualização automática, Atualização inicial, Atualização de máquina ou Atualização de correções. Uma Varredura de correções detecta correções que estão faltando e estão instaladas em uma máquina e, portanto, decide como proceder com a estratégia de correção que pode ser tomada. Correções que são detectadas por uma Varredura de correções são apresentadas em uma variedade de Políticas de correções, que poderão, então, ser usadas para controlar quais correções estão aprovadas para implementação em máquinas. As Atualizações automáticas implementam correções aprovadas em máquinas mediante agendamento e com base em sua participação na Política de correções. Atualizações iniciais, Atualizações em máquinas e Atualizações de correções fornecem capacidades de agendamento manuais ou individuais para a estratégia geral de correções. Para manter informações de status de correções disponíveis sobre máquinas atualizadas para que decisões de implementação e aprovação possam ser tomadas em relação à correção, é importante agendar as auditorias de varreduras de correções em um padrão de certa forma recorrente regularmente. A implementação de correções de forma regular também é essencial para os objetivos do Patch Management; portanto, o agendamento de Atualizações automáticas também é importante. Com o uso de conteúdo do Patch Management, essas tarefas recorrentes podem ser agendadas. O conteúdo do Patch Management também inclui um conjunto de Políticas de correções para o qual diferentes máquinas podem ser atribuídas, seja automaticamente ou manualmente. Com essa estratégia do Patch Management, haverá formas fáceis de localizar sistemas específicos com base nos detalhes de correções instaladas e/ou ausentes, quantidade de correções ausentes, máquinas em determinadas Políticas de correções, bem como haverá como gerar relatórios e atuar com eficácia em relação a esses grupos de máquinas, se necessário. O conteúdo adicional fornecido com o pacote oferece certo suporte básico para Atualizações de software Macintosh e Atualizações/upgrades de pacote Linux.

Políticas

É fornecido um conjunto de Políticas que aplicam agendamentos recorrentes de Varredura de correções e Atualização automática nas máquinas com Windows compatíveis na infraestrutura de TI. Essas políticas permitem a detecção recorrente de correções que são instaladas e ausentes em todas as máquinas, bem como o agendamento de implementação de correções aprovadas. Também são incluídas políticas para atribuir servidores e estações de trabalho com Windows às Políticas de correções apropriadas, bem como para oferecer suporte à não correção de determinadas máquinas ou configuração de um grupo de teste para implementação de correções antes de uma aprovação geral e implementação de novas correções. É fornecida uma política adicional que aplica agendamentos recorrentes de Atualização de software Macintosh nas máquinas Macintosh compatíveis com a infraestrutura de TI.

As políticas incluídas estão localizadas em **[System].Core.Org Specific Policies.Patch / Update Management** e são descritas a seguir.

- **Windows.Common Windows Patch Mgmt Settings**
    - **Configurações de negação de correção**: aplica configurações de gerenciamento de correções em máquinas selecionadas na visualização 'zz[SYS] Policy - Patch_Deny Patching Group'. Define a Ação de reinicialização como "Não reinicializar após a atualização". Define a participação na Política de correções como a política de correções "Recusar correções". Define Alertas de correção para gerar um Alarme e enviar um e-mail para o endereço de e-mail de "Alertas de correção" quando houver "Falha na instalação da correção" ou "A credencial do agente é inválida ou está ausente".
    - **Configurações de negação de correção**: aplica configurações de gerenciamento de correções em máquinas selecionadas na visualização 'zz[SYS] Policy - Patch_Test Patching Group'. Define a Ação de reinicialização como "Se o usuário estiver conectado, solicitar a reinicialização a cada 60 minutos até que esta ocorra. Reinicializar se o usuário não estiver conectado". Define a participação na Política de correções como a política de correções

"Testar correções". Define Alertas de correção para gerar um Alarme e enviar um e-mail para o endereço de e-mail de "Alertas de correção" quando houver "Falha na instalação da correção" ou "A credencial do agente é inválida ou está ausente".

- **Desativar atualização automática do Windows**: desativa atualizações automáticas do Windows em máquinas que têm a Atualização automática do Windows ativada. Se a Atualização automática do Windows estiver ativada e o Kaseya Patch Management estiver sendo usado, então poderá haver um conflito da Atualização automática do Windows com a estratégia de gerenciamento de correções Kaseya, podendo resultar na implementação de correções que foram negadas ou que ainda estejam com aprovação pendente no Kaseya.
- **Origem do arquivo - Internet**: define a origem de arquivo do Patch Management como Internet para todas as máquinas com Windows, a fim de que as correções sejam obtidas por download diretamente dos servidores de correções e download da Microsoft. Essa política é o padrão e pode ser substituída por uma política alternativa que é aplicada a organizações ou grupos de máquinas específicas; também tem precedência sobre essa política.

- **Windows.Windows Workstation Patch Mgmt Settings**
  - **Configurações de correções de estação de trabalho**: aplica configurações do Patch Management a estações de trabalho com Windows. Define a Ação de reinicialização como "Se o usuário estiver conectado, solicitar a reinicialização a cada 60 minutos até que esta ocorra. Reinicializar se o usuário não estiver conectado". Define a participação na Política de correções como a política de correções "Correções da estação de trabalho". Define Alertas de correção para gerar um Alarme e enviar um e-mail para o endereço de e-mail de "Alertas de correção" quando houver "Falha na instalação da correção" ou "A credencial do agente é inválida ou está ausente".
  - **Agendamento diário de estação de trabalho para mais de 10 correções (atualização automática, de segunda a sexta, das 6h às 18h/gestão de energia)**: aplica agendamentos diários de atualização automática a membros da Política de correções de estação de trabalho que estão com 10 ou mais correções aprovadas ausentes. As atualizações automáticas estão agendadas para ocorrer de segunda a sexta, semanalmente, das 6h às 18h. Essa política geralmente é usada quando clientes têm máquinas que estão com algumas correções ausentes e eles querem que esses sistemas sejam atualizados ao longo de dias, em vez de semanas ou meses. Assim que as máquinas forem corrigidas não precisarão mais ter correções aplicadas diariamente. As atualizações automáticas são realizadas durante o dia para atender a clientes nos quais as máquinas geralmente são desligadas à noite, mas a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas durante o dia possam ser ativadas antes da realização dessas operações.
  - **Agendamento semanal de estação de trabalho (varredura, às terças-feiras, das 6h às 18h/Atualização automática, às quartas-feiras, das 6h às 18h/gestão de energia)**: aplica agendamentos semanais de atualização automática e varredura de correções a membros da Política de correções de estação de trabalho. As varreduras de correção estão agendadas para que ocorram às terças-feiras, semanalmente, das 6h às 18h, e as atualizações automáticas estão agendadas para às quartas-feiras, semanalmente, das 6h às 18h. Essa política geralmente é usada quando clientes querem usar uma abordagem mais agressiva para correções, a fim de ajudar a minimizar riscos devido ao fato de máquinas não serem corrigidas e, portanto, querem que novas correções sejam implementadas relativamente rápido em máquinas. As atualizações automáticas são realizadas durante o dia para atender a clientes nos quais as máquinas geralmente são desligadas à noite, mas a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas durante o dia possam ser ativadas antes da realização dessas operações.
- **Windows.Windows Server Patch Mgmt Settings**
  - **Configurações de correções de servidor**: aplica configurações do Patch Management a servidores com Windows. Define a Ação de reinicialização como "Não reinicializar após a atualização", "Quando for necessário reinicializar, enviar um e-mail para 'Alertas de correção'". Define a participação na Política de correções como a política de correções "Correções do servidor". Define Alertas de correção para gerar um Alarme e enviar um

e-mail para o endereço de e-mail de "Alertas de correção" quando houver "Falha na instalação da correção" ou "A credencial do agente é inválida ou está ausente".

- **Agendamento semanal de servidor (varredura, semanal, das 18h às 6h)**: aplica agendamento de varredura de correção a membros da política de correção de servidor. Varreduras de correção são agendadas para ocorrer às quartas-feiras, semanalmente, das 18h às 6h. Nenhuma implementação de atualização automática está agendada em servidores por esta política.

- **Macintosh.Macintosh Workstation Software Update Settings**
  - **Atualização semanal de software de estação de trabalho Macintosh (instalação recomendada, às quartas-feiras, das 18h às 6h)**: aplica uma atualização de software Mac para execução às quartas-feiras, todas as semanas, que instalará atualizações de software Macintosh recomendadas em estações de trabalho Macintosh. As atualizações de software são realizadas durante o dia para atender a clientes nos quais as máquinas geralmente são desligadas à noite, mas a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas durante o dia possam ser ativadas antes da realização dessas operações.

Políticas de aprovação/negação de correções

> **Nota:** "Políticas" de aprovação/negação de correções são um tipo especializado de política no módulo Patch Management que não deve ser confundido com políticas definidas usando o módulo **Policy Management**. Foram criadas políticas do **Policy Management** que especificam políticas de aprovação/negação de correções predefinidas.

Um conjunto de políticas de correção predefinido é fornecido para controlar a aprovação e a negação de várias correções para Windows aplicáveis aos sistemas operacionais Windows e software Microsoft compatíveis.

Nome da política de correções	**Descrição**
zz[SYS] Deny Patching	Usado para negar todas as correções em casos em que máquinas não devem ser corrigidas por motivos específicos. O status de aprovação padrão para novas correções de todas as classificações de segurança da Microsoft está definido como Negado. Para obter mais informações sobre como máquinas podem ser atribuídas a esta política de correções, consulte Como gerenciar participações em política de correções.
zz[SYS] Server Patching	Usado para aprovação e negação de correções para servidores Windows. O status de aprovação padrão para novas correções de todas as classificações de segurança da Microsoft está definido como Aprovação pendente. Todos os servidores Windows se tornam membros desta Política de correções quando Gerenciamento de correções de servidor é ativado através do Gerenciamento automatizado de sistemas.
zz[SYS] Test Patching	Usado para aprovação e negação de correções para máquinas que serão usadas para testes de correções antes da implementação geral em servidores e estações de trabalho Windows. O status de aprovação padrão para novas atualizações críticas e de segurança de alta prioridade com base em suas classificações de segurança da Microsoft está definido como Aprovado. Todos os servidores Windows se tornam membros desta Política de correções quando Gerenciamento de correções de servidor é ativado através do Gerenciamento automatizado de sistemas. Para obter mais informações sobre como máquinas podem ser atribuídas a esta política de correções, consulte Como gerenciar participações em política de correções.
zz[SYS] Workstation Patching	Usado para aprovação e negação de correções para estações de trabalho Windows. O status de aprovação padrão para novas atualizações críticas

	e de segurança de alta prioridade com base em suas classificações de segurança da Microsoft está definido como Aprovado. Todas as estações de trabalho Windows se tornam membros desta Política de correções quando o Gerenciamento de correções de estação de trabalho é ativado através do Gerenciamento automatizado de sistemas.

Vistas

Uma variedade de visualizações predefinida é fornecida e pode ser usada em todos os aspectos do gerenciamento de serviços de TI, bem como para suporte ao serviço de gerenciamento de correções/atualizações. Essas visualizações fornecem a capacidade de filtrar máquinas no sistema com base na configuração de correções, na quantidade de correções ausentes, no status de reinicialização de correções e na participação em políticas de correções, entre outras. As visualizações a seguir podem ser usadas em atividades de geração de relatórios e operacionais.

Visualizar nome	Descrição
zz[SYS] Patch - Deny Patching Policy	Exibe todas as máquinas atribuídas como membros para a política de correções "zz[SYS] - Deny Patching".
zz[SYS] Patch - Missing 10+ Approved Patches	Exibe todas as máquinas que estão com 10 ou mais correções aprovadas ausentes com base nas participações de políticas de correções de máquinas e as correções aprovadas nessas políticas.
zz[SYS] Patch - Missing 20+ Approved Patches	Exibe todas as máquinas que estão com 20 ou mais correções aprovadas ausentes com base nas participações de políticas de correções de máquinas e as correções aprovadas nessas políticas.
zz[SYS] Patch - No Policy	Exibe todas as máquinas que não estão atribuídas a políticas de correções.
zz[SYS] Patch - Pending Reboot	Exibe todas as máquinas com uma reinicialização relacionada à implementação de correção pendente.
zz[SYS] Patch - Scan Failed	Exibe todas as máquinas nas quais a última varredura de correção falhou por algum motivo.
zz[SYS] Patch - Scan Not Scheduled	Exibe todas as máquinas que não tiveram uma varredura de correção agendada.
zz[SYS] Patch - Server Patching Policy	Exibe todas as máquinas que são membros da política de correções "zz[SYS] - Server Patching".
zz[SYS] Patch - Servers w No Policy	Exibe todas as máquinas de servidor que não estão atribuídas a políticas de correções.
zz[SYS] Patch - Test Patching Policy	Exibe todas as máquinas que são membros da política de correções "zz[SYS] Test Patching".
zz[SYS] Patch - Windows Auto Update Enabled	Exibe todas as máquinas com atualização automática do Windows ativada com base no que foi detectado durante a última varredura de correção.
zz[SYS] Patch - Workstation Patching Policy	Exibe todas as máquinas que são membros da política de correções "zz[SYS] - Workstation Patching".
zz[SYS] Patch - Workstations w No Policy	Exibe todas as máquinas de estações de trabalho que não estão atribuídas a políticas de correções.

Procedimentos do agente

São fornecidos procedimentos de agente que realizam automação personalizada em suporte ao serviço de gerenciamento de TI de correções/atualizações. Esses procedimentos de agente estão localizados sob o gabinete **Sistema** da página Procedimentos do agente > **Agendar/Criar** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2845.htm)*.

- **Criar ponto de restauração do sistema de gerenciamento de correções**: essa opção é executada como um pré-procedimento para atualizações automáticas. Pontos de restauração podem ser usados durante uma recuperação caso uma correção/atualização instalada cause problemas.
  - **Localização:** System.Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore.Create Patch Management System Restore Point
  - **Descrição:** usa WMIC para criar um ponto de restauração do sistema denominado Gerenciamento de correções. Este procedimento do agente pode ser chamado antes de uma implementação de correção através de um procedimento do pré-agente de atualização automática.
  - **Executar por política:** System.Core.Org Specific Policies.Patch/Update Management.Windows Workstation Patch Settings.Workstation Patch Settings
- **Atualização de software Mac: instalar atualizações recomendadas e recuperar/registrar resultados em logs**
  - **Localização:** System.Core.2 Macintosh Procedures.Software Update.Mac Software Update - Install Recommended Updates and Retrieve/Log Results
  - **Descrição:** instala atualizações de software Mac recomendadas.
  - **Executar por política:** System.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Workstation Software Update Settings.Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6pm-6am)

Manutenção de rotina

Objetivo

Fornecer uma estratégia de manutenção de rotina para máquinas gerenciadas para incluir otimização do sistema, bem como operações de manutenção preventiva, como limpeza de disco e arquivos temporários, análise de disco rígido, reparo e otimização, e muito mais. A manutenção de rotina é vital para ajudar a garantir que sistemas sejam executados sem problemas e operem em seu potencial de desempenho de pico. Instituir um agendamento de manutenção de rotina automatizada básica em sistemas compatíveis inicialmente com foco em estações de trabalho, mas extensível e com capacidade de suporte para operações de manutenção mais avançadas ao longo do tempo, bem como servidores, conforme necessário.

Visão geral

A automação da Kaseya intitulada Procedimentos do agente pode ser usada para realizar praticamente qualquer tarefa em um ou mais sistemas com base em agendamentos. Tarefas automáticas como verificação de discos, análise de fragmentação e otimização de disco, reparos de volume, limpeza interna, limpeza de caches, limpeza de arquivos temporários, rotação de logs e muito mais são combinadas em uma avançada solução de manutenção de rotina que é aplicada a estações de trabalho Windows e Macintosh para manter esses sistemas funcionando perfeitamente.

Políticas

Um conjunto de Políticas que aplicam agendamentos recorrentes de manutenção de rotina em estações de trabalho Windows e Macintosh. Essas políticas, por sua vez, fazem com que procedimentos do agente realizem a manutenção em cada sistema em horários agendados regularmente. As políticas incluídas estão localizadas em **[System].Core.Org Specific Policies.Routine Maintenance** e são descritas a seguir.

- **Manutenção recorrente de estação de trabalho Windows**
  - **Manutenção de estação de trabalho Windows (semanal, de segunda a sexta, das 18h às 6h)**: aplica um procedimento de manutenção de estação de trabalho Windows agendado para execução a todas as máquinas de estação de trabalho Windows, semanalmente (de segunda a sexta), das 18h às 6h. Se a máquina não estiver ligada quando a manutenção for agendada, então

a máquina ignorará esse ciclo de manutenção e tentará executar a manutenção novamente uma semana depois.

- **Manutenção recorrente de estação de trabalho Macintosh**
  - **Agendamento de manutenção de estação de trabalho Macintosh (semanal, de segunda a sexta, das 18h às 6h)**: aplica um procedimento de manutenção de estação de trabalho Macintosh agendado para execução a todas as máquinas de estação de trabalho Macintosh, semanalmente (de segunda a sexta), das 18h às 6h. Se a máquina não estiver ligada quando a manutenção for agendada, então a máquina ignorará esse ciclo de manutenção e tentará executar a manutenção novamente uma semana depois.

Procedimentos do agente

Um conjunto de Procedimentos do agente realizará vários aspectos das tarefas de manutenção em estações de trabalho Windows e Macintosh. Esses procedimentos são agendados via Política para execução em um agendamento recorrente. Os procedimentos do agente incluídos estão localizados em **[System].Core** e são descritos a seguir.

- **1 Windows Procedures.Desktops.Maintenance.Desktop Maintenance.Workstation Weekly Maintenance**
  - **Descrição:** executa todas as tarefas de manutenção de desktop semanalmente; agende este script para execução durante o intervalo de manutenção.
  - **Uso:** agendado por gerenciamento de políticas para execução em todas as estações de trabalho Windows, semanalmente (de segunda a sexta), das 18h às 6h através da Política "Manutenção de estação de trabalho Windows (semanal, de segunda a sexta, das 18h às 6h)" quando o recurso Manutenção da estação de trabalho estiver ativado via Gerenciamento automatizado de sistemas.
- **Common Maintenance Tasks.System Restore.Create Weekly Desktop Maintenance System Restore Point**
  - **Descrição:** usa WMIC para criar um ponto de restauração do sistema chamado de manutenção semanal de desktop. Este procedimento do agente pode ser acionado no início do procedimento de manutenção semanal da estação de trabalho.
  - **Uso:** acionado pelo procedimento de manutenção semanal da estação de trabalho.
- **Common Maintenance Tasks.Flush DNS. Descarregar cache de resolvedor DNS**
  - **Descrição:** descarrega e redefine o conteúdo do cache do resolvedor de cliente DNS ao executar o comando IPCONFIG /FLUSHDNS.
  - **Uso:** acionado pelo procedimento de manutenção semanal da estação de trabalho.
- **Common Maintenance Tasks.IE Files Management. Limpar arquivos temporários do Internet Explorer**
  - **Descrição:** limpa os arquivos temporários do Internet Explorer do usuário atualmente conectado.
  - **Uso:** acionado pelo procedimento de manutenção semanal da estação de trabalho.
- **Common Maintenance Tasks.TEMP Files.Clear User TEMP Folder**
  - **Descrição:** exclui todos os arquivos e pastas na pasta %TEMP%, e sob ela, dos usuários conectados que não estão atualmente bloqueados/abertos pelo Windows.
  - **Uso:** acionado pelo procedimento de manutenção semanal da estação de trabalho.
- **Common Maintenance Tasks.Disk Cleanup.Windows Disk Cleanup**
  - **Descrição:** define as entradas do registro "sageset" para o cleanmgr.exe e então executa o cleanmgr.exe com o parâmetro "sagerun" para limpar automaticamente os arquivos nas seguintes localizações: Active Setup Temp Folder Content Indexer Cleaner Downloaded Program Files Internet Cache Files Memory Dump Files Old ChkDsk Files Recycle Bin Remote Desktop Cache Files Setup Log Files Temporary Files Temporary Offline Files WebClient e WebPublisher Cache.
  - **Uso:** acionado pelo procedimento de manutenção semanal da estação de trabalho.
- **Common Maintenance Tasks.Check Disk.Check Disk System Drive (Schedule at Next Restart)**

- **Descrição:** executa um comando CHKDSK na unidade do sistema. Os resultados da manutenção são avaliados pelo script de verificação de disco.
- **Uso:** acionado pelo procedimento de manutenção semanal da estação de trabalho.

- **Common Maintenance Tasks.Defragmentation.Defragment System Drive (Analysis & Prompt User If Reqd)**
  - **Descrição:** realiza uma análise de desfragmentação na unidade do sistema no Windows (geralmente, C:). Os resultados de desfragmentação são gravados no log de procedimentos do agente. Se um usuário estiver conectado na máquina, então o procedimento perguntará se ele deseja executar uma desfragmentação completa na unidade e realizará uma se a resposta for sim.
  - **Uso:** acionado pelo procedimento de manutenção semanal da estação de trabalho.
- **2 Macintosh Procedures.Maintenance.Macintosh Weekly Maintenance**
  - **Descrição:** realiza várias tarefas de manutenção de roteamento em uma máquina com Macintosh OS X.
  - **Uso:** agendado por gerenciamento de políticas para execução em todas as estações de trabalho Macintosh, semanalmente (de segunda a sexta), das 18h às 6h através da Política "Manutenção de estação de trabalho Macintosh (semanal, de segunda a sexta, das 18h às 6h)" quando o recurso Manutenção da estação de trabalho estiver ativado via Gerenciamento automatizado de sistemas.
- **Limpeza geral de máquina com OS X**
  - **Descrição:** realiza limpeza do sistema, remove arquivos de log antigos, arquivos "scratch" e "junk", limpa caches do sistema e do usuário, faz a rotatividade de logs de sistema e aplicativos, recria cache DYLD e recria o índice Spotlight.
  - **Uso:** acionado pelo procedimento de manutenção semanal do Macintosh.
- **Verificar e reparar volumes de disco do OS X**
  - **Descrição:** realiza operações de reparo e verificação de disco usando DISKUTIL.
  - **Uso:**acionado pelo procedimento de manutenção semanal do Macintosh.
- **Reparar permissões de disco do OS X**
  - **Descrição:** realiza uma operação de permissões de reparo de disco usando DISKUTIL.
  - **Uso:**acionado pelo procedimento de manutenção semanal do Macintosh.

Monitoramento

Nesta seção

Visão geral de recursos de monitoramento

Objetivo

Fornecer uma estratégia de monitoramento para monitorar e emitir alertas sobre ativos de hardware e software. O monitoramento de eventos fundamentais do sistema em servidores Windows em tempo hábil, sete dias por semana, garante a integridade de sua infraestrutura de TI. Se um problema estiver prestes a ocorrer, a falha em ser notificado imediatamente poderia afetar materialmente o impacto da continuidade de seus negócios. Como as máquinas na infraestrutura de TI compatível mudam ao longo do tempo, o monitoramento deve tentar selecionar essas alterações e iniciar o monitoramento devidamente com base nessas alterações.

Visão geral

O monitoramento da Kaseya fornece várias formas de monitoramento de sistemas com agente e sem agente na infraestrutura de TI compatível de clientes. O monitoramento da disponibilidade de servidor na forma de alertas de status do agente fornece notificações quando sistemas ficam inativos ou estão "off-line" devido a causas importantes, como falhas, reinicializações, conectividade de rede, sobrecarga do sistema etc. O monitoramento do serviço Windows na forma de conjuntos de monitor com verificações de serviço fornece monitoramento contínuo de serviços Windows importantes, bem como envia notificações e realiza correção automática (serviços de reinicialização) quando esses serviços não estão em execução/são interrompidos. O monitoramento de logs de eventos na forma de alertas do conjunto de eventos fornece monitoramento contínuo de logs de eventos do Windows, bem como envia notificações quando eventos importantes são registrados em log nesses conjuntos de eventos de log do Windows. O monitoramento de desempenho na forma de conjuntos de monitores com limites do contador fornece monitoramento contínuo de importantes contadores de desempenho do Windows, bem como envia notificações quando os valores dos contadores atendem a determinados limites onde poderia haver um impacto negativo no desempenho, na disponibilidade e/ou na confiabilidade do sistema. O monitoramento de status, eventos e valores de contadores é registrado no sistema para fins de atualização de histórico, tendências e geração de relatórios. Alarmes gerados por sistemas de monitoramento são registrados em log no sistema para fins de histórico e geração de relatórios. São aceitos vários níveis de gravidade para que problemas que surjam possam ser priorizados devidamente e as partes corretas notificadas por e-mail.

A visão geral de recursos de monitoramento a seguir detalha os tipos de sistema e monitoramento incluídos no pacote de solução padrão.

Tipos de monitoramento = (A=Availability (Disponibilidade), E=Event Log (Log de eventos), S=Services (Serviços), P=Performance (Desempenho)

Tipo de sistema (Categoria)	Tipos de monitoramento	Visão geral de monitoramento
Todos os servidores Windows (SO)	AESP	Core Win Srvr Monitoring
Windows Server 2003 (OS)	--S-	Win 2003 Services
Windows Server 2008/2008 R2 (OS)	--S-	Win 2008/2008R2 Services

Todas as estações de trabalho Windows (SO)	AESP	Core Win Wkst Monitoring
Windows Vista (SO)	--S-	Win Vista Services
Windows 7 (SO)	--S-	Win 7 Services
Windows XP (SO)	--S-	Win XP Services
Dell PowerEdge (Hardware)	-E--	Dell PowerEdge HW Events
HP ProLiant (Hardware)	-E--	HP ProLiant HW Events
IBM Series x (Server Hardware)	-E--	IBM Series x HW Events
Backup Exec Server (Role)	-ES-	Backup Exec Monitoring
Blackberry Enterprise Server	-ESP	Blackberry Server Monitoring
BrightStor ARCServe Server	-ES-	BrightStor Server Monitoring
Citrix Server	-ES-	Citrix Server Monitoring
Servidor DHCP	-ESP	DHCP Server Monitoring
Servidor DNS	-ESP	DNS Server Monitoring
Domain Controller (Network Infra)	-ESP	DC/AD Monitoring
Exchange 2003 Server (Email)	-ES-	Exch 2003 Monitoring
Exchange 2007 Server (Email)	-ES-	Exch 2007 Monitoring
Exchange 2010 Server (Email)	-ESP	Exch 2010 Monitoring
Exchange Server (Email)	-ESP	Core Exchange Monitoring
File Server (File/Print)	--S-	File Server Monitoring
FTP Server (Web Systems)	--S-	FTP Server Monitoring
IIS Server (Web Systems)	-ESP	IIS Server Monitoring
IMAP4 Server (Email)	--S-	IMAP4 Server Monitoring
POP3 Server (Email)	--S-	POP3 Server Monitoring
Print Server (File/Print)	-ESP	Print Server Monitoring
Microsoft SE-FEP (Security)	-ES-	Microsoft SE-FEP Monitoring
SharePoint Server (Web Systems)	--S-	SharePoint Server Monitoring
SMTP Server (Email)	-ESP	SMTP Server Monitoring
SQL Server (Database)	--SP	Core SQL Server Monitoring
SQL Server 2005 (Database)	--S-	SQL Server 2005 Monitoring
SQL Server 2008 (Database)	--S-	SQL Server 2008 Monitoring
Terminal Server (Remote Access)	-ESP	Terminal Server Monitoring
WINS Server (Network Infra)	--S-	WINS Server Monitoring
AVG Tech (Security)	--S-	AVG Tech AV Monitoring
Kaspersky ES (Security)	--S-	Kaspersky ES Monitoring
McAfee (Security)	-ES-	McAfee Monitoring
Sophos (Security)	-ES-	Sophos Monitoring
Symantec AV (Security)	-ES-	Symantec AV Monitoring
Symantec EP (Security)	-ES-	McAfee AV Monitoring
Trend Micro (Security)	-ES-	McAfee AV Monitoring

Monitoring Severity Matrix

		Ações de monitoramento

Nível de gravidade	Descrição	E-mail	Alarme	Rearmar
Gravidade 0	Informações/Registro em logs	Não	Não	N/D
Gravidade 1	Baixo impacto/risco	Sim	Sim	7 dias
Gravidade 2	Impacto médio/	Sim	Sim	1 Dias
Gravidade 3	Alto impacto/risco	Sim	Sim	12 horas
Alerta fixo	Alto impacto/risco	Sim	Sim	12 horas

Nota: Níveis de gravidade se aplicam somente a conjuntos de monitores e conjuntos de eventos, e são designados no nome do conjunto. Os alertas fixos são todos configurados para se comportarem como gravidade 3.

Políticas de monitoramento

Uma variedade de políticas aplicam configurações específicas de *monitoramento* a máquinas com base em seu sistema operacional e versão do Windows, hardware, função e produtos de segurança/antivírus. Essas políticas permitem o uso de vários componentes de monitoramento de desempenho, serviço, log de eventos e disponibilidade, bem como automação de monitoramento relacionada. As políticas incluídas estão localizadas em **[System].Core.Org Specific Policies.Monitoring** e são descritas a seguir.

Nesta seção

Servidor

- **Monitoramento comum do Windows Server**: aplica um conjunto comum de monitoramento para todos os servidores Windows. Isso inclui log de eventos relacionados a hardware, Windows Service e monitoramento comum de desempenho do Windows.
- **Windows Server (Core)**: aplica uma variedade de monitoramentos do Windows Server (Core) a Windows Servers, incluindo monitoramento de serviços padrão, desempenho do sistema, geração de relatórios de integridade, logs de eventos e muito mais.
- **Windows Server 2003**: aplica monitoramento de serviço padrão para Windows 2003 Servers.
- **Windows Server 2008/2008 R2**: aplica monitoramento de serviço padrão para Windows 2008/2008 R2 Servers.

Hardware

- **Dell PowerEdge**: aplica alertas e monitoramento específicos a hardware de servidor Dell PowerEdge. Esse monitoramento pode exigir que ferramentas específicas de monitoramento de servidor Dell PowerEdge sejam instaladas na máquina do servidor.
- **HP ProLiant**: aplica alertas e monitoramento específicos a hardware de servidor HP ProLiant. Esse monitoramento pode exigir que ferramentas específicas de monitoramento de servidor HP ProLiant sejam instaladas na máquina do servidor.
- **IBM Series x**: aplica alertas e monitoramento específicos a hardware de servidor IBM Series X. Esse monitoramento pode exigir que ferramentas específicas de monitoramento de servidor IBM Series X sejam instaladas na máquina do servidor.

Funções

- **Backup Exec Server**: aplica monitoramento a servidores de execução de backup.
- **Blackberry Enterprise Server**: aplica monitoramento a servidores Blackberry Enterprise.
- **BrightStor ARCServe Server**: aplica monitoramento a servidores BrightStor.
- **Citrix Server**: aplica monitoramento a servidores Citrix.
- **DHCP Server**: aplica monitoramento a servidores DHCP.
- **DNS Server**: aplica monitoramento a servidores DNS.
- **Domain Controller**: aplica monitoramento a controladores de domínio.
- **Exchange 2003 Server**: aplica monitoramento a servidores Exchange 2003.

- **Exchange 2007 Server**: aplica monitoramento a servidores Exchange 2007.
- **Exchange 2010 Server**: aplica monitoramento a servidores Exchange 2010.
- **Exchange Server**: aplica monitoramento a servidores Exchange.
- **File Server**: aplica monitoramento a servidores de arquivos.
- **FTP Server**: aplica monitoramento a servidores de FTP.
- **IIS Server**: aplica monitoramento a servidores ISS.
- **IMAP4 Server**: aplica monitoramento a servidores IMAP4.
- **POP3 Server**: aplica monitoramento a servidores POP3.
- **Print Server**: aplica monitoramento a servidores de impressão.
- **SharePoint Server**: aplica monitoramento a servidores SharePoint.
- **SMTP Server**: aplica monitoramento a servidores SMTP.
- **SQL Server**: aplica monitoramento a servidores SQL.
- **SQL Server 2005**: aplica monitoramento a servidores SQL 2005.
- **SQL Server 2008**: aplica monitoramento a servidores SQL 2008.
- **Terminal Server**: aplica monitoramento a servidores de Terminal.
- **WINS Server**: aplica monitoramento a servidores WINS.

Estação de trabalho

- **Monitoramento comum de estação de trabalho com Windows**: aplica um conjunto comum de monitoramento para todas as estações de trabalho com Windows. Isso inclui log de eventos relacionados a hardware, Windows Service e monitoramento comum de desempenho do Windows.
- **Estação de trabalho com Windows (Core)**: aplica uma variedade de monitoramentos de estações de trabalho com Windows (Core) a estações de trabalho com Windows, incluindo monitoramento de serviços padrão, desempenho do sistema, geração de relatórios de integridade e muito mais.
- **Windows Vista**: aplica monitoramento de serviço padrão para máquinas com Windows Vista.
- **Windows 7**: aplica monitoramento de serviço padrão para máquinas com Windows 7.
- **Windows XP**: aplica monitoramento de serviço padrão para máquinas com Windows XP.

Security.Antivirus

- **AVG Tech**: aplica monitoramento do AVG Technologies AntiVirus.
- **McAfee**: aplica monitoramento do McAfee AntiVirus.
- **Microsoft SE-FEP**: aplica monitoramento do Microsoft Security Essentials e Forefront Endpoint Protection.
- **Sophos**: aplica monitoramento do Sophos AntiVirus.
- **Symantec AV**: aplica monitoramento do Symantec AntiVirus.
- **Symantec EP**: aplica monitoramento do Symantec Endpoint Protection AntiVirus.
- **Trend Micro**: aplica monitoramento do Trend Micro AntiVirus.

Utilitário

- **Atualizar listas por varredura**: aplica uma atualização de listas por varredura agendada em todas as máquinas com Windows para manter informações de serviços de execução, log de eventos e contador de desempenho atualizadas para cada máquina para fins de monitoramento preciso.
- **Limpeza de monitoramento**: como a última política que contém conjuntos de monitores e alertas, essa política garante efetivamente que o monitoramento aplicado anteriormente (conjuntos de monitores e alertas de logs de eventos atribuídos através de outras políticas não mais necessários devido a alterações de função etc.) seja removido.

Conjuntos de monitores

Uma variedade de conjuntos de monitores são fornecidos e aplicados através de políticas relacionadas a monitoramento. Esses conjuntos de monitores monitoram contadores de desempenho e Windows Services usando limites do contador e verificações de serviço. Os conjuntos de monitores fornecidos incluem monitoramento de serviços de SO Windows importantes e serviços para sistemas Microsoft comuns, como Active Directory, Exchange, SQL, IIS e muito mais. Monitoramento de desempenho de sistema básico para espaço em disco, utilização de memória, utilização de CPU, bem como monitoramento mais avançado de desempenho específico do sistema estão incluídos. Os conjuntos de monitores incluídos estão localizados em **[System].Core** e são descritos a seguir.

Nesta seção

Backup

- **Backup - Backup Exec Continuous Protection Services - {Severity3}**
  - Monitora serviços de proteção contínua de execução de backup em servidores de execução de backup. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Backup - Backup Exec DLO Agent Services - {Severity3}**
  - Monitora serviços de agente DLO de execução de backup em servidores de execução de backup. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Backup - Backup Exec Services - {Severity3}**
  - Monitora serviços de execução de backup em servidores de execução de backup. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Backup - Backup Exec System Recovery Service - {Severity3}**
  - Monitora serviço de recuperação de execução de backup em servidores de execução de backup. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Backup - BrightStor ARCServe Backup Services - {Severity3}**
  - Monitora serviços de backup do BrightStor ARCServe em servidores de backup BrightStor ARCServe. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Banco de dados

- **Database - SQL Server (All Instances) Services - {Severity3}**

- Monitora serviços SQL Server em servidores SQL Server usando o serviço MSSQL* de caractere curinga. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

- **Database - SQL Server (Default Instance) - {Severity0}**
  - Coleta contadores de desempenho do servidor SQL (instância padrão) em servidores SQL. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Database - SQL Server (Default Instance) Performance - {Severity2}**
  - Monitora desempenho do servidor SQL (instância padrão) em servidores SQL. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Database - SQL Server (Default Instance) Services - {Severity3}**
  - Monitora serviços do servidor SQL (instância padrão) em servidores SQL. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Database - SQL Server 2005 Optional Services - {Severity3}**
  - Monitora serviços opcionais de SQL Server 2005 em servidores SQL Server 2005. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Database - SQL Server 2005 Services - {Severity3}**
  - Monitora serviços de SQL Server 2005 em servidores SQL Server 2005. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Database - SQL Server 2008 Optional Services - {Severity3}**
  - Monitora serviços opcionais de SQL Server 2008 em servidores SQL Server 2008. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Database - SQL Server 2008 Services - {Severity3}**
  - Monitora serviços de SQL Server 2008 em servidores SQL Server 2008. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

E-mail

- **Email - Blackberry Server Performance - {Severity2}**
  - Monitora desempenho de Blackberry Server em servidores Blackberry. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Email - BlackBerry Server Services - {Severity3}**
  - Monitora serviços dos servidores Blackberry Server em servidores Blackberry. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange 2003 Services - {Severity3}**
  - Monitora serviços do Exchange 2003 em servidores Exchange 2003. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange 2007 Services - {Severity3}**
  - Monitora serviços do Exchange 2007 em servidores Exchange 2007. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange 2010 Edge Transport Queues - {Severity0}**

- Coleta contadores de desempenho de filas de transporte de borda do Exchange 2010 em servidores Exchange 2010. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity2}**
  - Monitora contadores de desempenho de filas de transporte de borda do Exchange 2010 em servidores Exchange 2010. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity3}**
  - Monitora contadores de desempenho de filas de transporte de borda do Exchange 2010 em servidores Exchange 2010. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange 2010 Services - {Severity3}**
  - Monitora serviços do Exchange 2010 em máquinas Exchange 2010. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange Client Active Logons - {Severity0}**
  - Coleta contador de desempenho de logons ativos de cliente Exchange em servidores Exchange. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Email - Exchange IMAP4 Service - {Severity3}**
  - Monitora serviço IMAP4 do Exchange em servidores Exchange. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange POP3 Service - {Severity3}**
  - Monitora serviço POP3 do Exchange em servidores Exchange. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange Server (Core) Performance - {Severity2}**
  - Monitora desempenho de servidor Exchange em servidores Exchange. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Email - Exchange Server (Core) Services - {Severity3}**
  - Monitora serviços do servidor Exchange (Core) em máquinas com Exchange Server (Core). Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange Server (Core) Store and Database - {Severity0}**
  - Coleta contadores de desempenho de banco de dados e loja do servidor Exchange em servidores Exchange. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Email - SMTP Queue Performance - {Severity3}**
  - Monitora o desempenho de fila SMTP em servidores SMTP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - SMTP Server Service - {Severity3}**
  - Monitora o serviço de servidor SMTP em servidores SMTP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Arquivo/impressão

- **File / Print - DFS Service - {Severity3}**
  - Monitora o serviço DFS em máquinas DFS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **File / Print - DFSR Service - {Severity3}**
  - Monitora o serviço DFSR em máquinas DFSR. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **File / Print - NTFRS Service - {Severity3}**
  - Monitora o serviço NTFRS em máquinas NTFRS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **File / Print - Print Queue Job Errors Performance - {Severity1}**
  - Monitora o desempenho de erros de trabalho da fila de impressão em servidores de arquivo e impressão. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **File / Print - Spooler Service - {Severity3}**
  - Monitora o serviço de spooler em serviços de arquivo e impressão. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Infraestrutura de rede

- **Network Infrastructure - Active Directory Domain Controller Services - {Severity3}**
  - Monitora serviços do controlador de domínio do Active Directory em controladores de domínio do Active Directory. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Network Infrastructure - DHCP Server Performance - {Severity2}**
  - Monitora desempenho de servidor DHCP em servidores DHCP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Network Infrastructure - DHCP Server Service - {Severity3}**
  - Monitora o serviço do servidor DHCP em servidores DHCP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Network Infrastructure - DNS Server Performance - {Severity2}**
  - Monitora desempenho de servidor DNS em servidores DNS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Network Infrastructure - DNS Server Service - {Severity3}**
  - Monitora o serviço de servidor DNS em servidores DNS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Network Infrastructure - WINS Server Service - {Severity3}**
  - Monitora o serviço do servidor WINS em servidores WINS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

OS Platforms.Windows (Core).Disk Space

- **Windows (Core) - Free Disk Space on Drive C - {Severity3}**

- Monitora o espaço livre em disco na unidade C em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

- **Windows (Core) - Free Disk Space on Drive D - {Severity3}**
  - Monitora o espaço livre em disco na unidade D em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Disk Space on Drive E - {Severity3}**
  - Monitora o espaço livre em disco na unidade E em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Disk Space on Drive F - {Severity3}**
  - Monitora o espaço livre em disco na unidade F em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Disk Space on Drive G - {Severity3}**
  - Monitora o espaço livre em disco na unidade G em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Space on C Drive Below 15 Percent - {Severity1}**
  - Monitora o espaço livre na unidade C abaixo de 15% em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Space on D Drive Below 15 Percent - {Severity1}**
  - Monitora o espaço livre na unidade D abaixo de 15% em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Space on E Drive Below 15 Percent - {Severity1}**
  - Monitora o espaço livre na unidade E abaixo de 15% em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Space on F Drive Below 15 Percent - {Severity1}**
  - Monitora o espaço livre na unidade F abaixo de 15% em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Space on G Drive Below 15 Percent - {Severity1}**
  - Monitora o espaço livre na unidade G abaixo de 15% em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.

OS Platforms.Windows (Core)

- **Windows (Core) - All Automatic Services - {Severity0}**
  - Coleta status de serviço de todos os serviços automáticos em máquinas com Windows. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Windows (Core) - CPU and Memory - {Severity0}**
  - Coleta contadores de desempenho de CPU e memória em máquinas com Windows. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Windows (Core) - Free Disk Space on Any Drive Below 1GB - {Severity2}**

- Monitora o espaço livre em disco em qualquer unidade abaixo de 1 GB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.

- **Windows (Core) - Free Disk Space on Any Drive Below 2GB - {Severity1}**
  - Monitora o espaço livre em disco em qualquer unidade abaixo de 2 GB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Disk Space on Any Drive Below 750MB - {Severity3}**
  - Monitora o espaço livre em disco em qualquer unidade abaixo de 750 MB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Disk Space on Drive C Below 1GB - {Severity2}**
  - Monitora o espaço livre em disco na unidade C abaixo de 1 GB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Windows (Core) - Free Disk Space on Drive C Below 2GB - {Severity1}**
  - Monitora o espaço livre em disco na unidade C abaixo de 2 GB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Disk Space on Drive C Below 750MB - {Severity3}**
  - Monitora o espaço livre em disco na unidade C abaixo de 750 MB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Machine Health - {Severity0}**
  - Coleta contadores de desempenho de integridade de máquina em máquinas com Windows. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Windows (Core) - Processor and Memory Performance - {Severity2}**
  - Monitora o desempenho do processador e memória em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Windows (Core) - TCPv4 Connections Performance - {Severity2}**
  - Monitora o desempenho de conexões TCPv4 em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.

Servidores Windows de plataformas de SO

- **Windows Server (Core) - Cluster Services - {Severity3}**
  - Monitora serviços de cluster em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows Server (Core) - Disk Time and Queue Length Performance - {Severity2}**
  - Monitora o desempenho de comprimento de fila e tempo de disco em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Windows Server (Core) - Drive C Performance - {Severity1}**
  - Monitora o desempenho da unidade C em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows Server (Core) - General System Performance - {Severity1}**

- Monitora o desempenho geral do sistema em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows Server (Core) - Server Reboots - {Severity1}**
  - Monitora reinicializações de servidor em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows Server (Core) - Standard Services - {Severity3}**
  - Monitora serviços padrão em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows Server 2003 - Standard Services - {Severity3}**
  - Monitora serviços padrão em máquinas com Windows Server 2003. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows Server 2008/2008 R2 - Standard Services - {Severity3}**
  - Monitora serviços padrão em máquinas com Windows Server 2008/2008 R2. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

OS Platforms.Windows Workstations

- **Windows 7 - Standard Services - {Severity1}**
  - Monitora serviços padrão em máquinas com Windows 7. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows Vista - Standard Services - {Severity1}**
  - Monitora serviços padrão em máquinas com Windows Vista. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows XP - Standard Services - {Severity1}**
  - Monitora serviços padrão em máquinas com Windows XP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.

Acesso remoto

- **Remote Access - Citrix Licensing Service - {Severity3}**
  - Monitora serviço de licenciamento Citrix em servidores Citrix. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Citrix Licensing WMI Service - {Severity3}**
  - Monitora serviço WMI de licenciamento Citrix em servidores Citrix. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Citrix MetaFrame Services - {Severity3}**
  - Monitora serviços Citrix MetaFrame em servidores Citrix. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Citrix Server Services - {Severity3}**

- Monitora serviços do servidor Citrix em servidores Citrix. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

- **Remote Access - Citrix Virtual Memory Optimization Service - {Severity3}**
  - Monitora serviço de otimização de memória virtual Citrix em servidores Citrix. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Terminal Server Services - {Severity3}**
  - Monitora serviços do Terminal Server em servidores de Terminal. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Terminal Server Session Performance - {Severity2}**
  - Monitora desempenho de sessão do Terminal Server em servidores de Terminal. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.

Segurança

- **AV - AVG Tech AVG Services - {Severity3}**
  - Monitora serviços AVG da AVG Tech em máquinas AVG da AVG Tech. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Kaspersky Endpoint Security Services {Severity3}**
  - Monitora serviços de segurança de endpoint Kaspersky em máquinas com Kaspersky Endpoint Security. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - McAfee Enterprise Services - {Severity3}**
  - Monitora serviços McAfee Enterprise em máquinas com McAfee Enterprise. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Sophos Antivirus Services - {Severity3}**
  - Monitora serviços da Sophos Antivirus em máquinas com Sophos Antivirus. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Symantec Antivirus Services - {Severity3}**
  - Monitora serviços da Symantec Antivirus em máquinas com Symantec Antivirus. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Symantec Endpoint Protection Services - {Severity3}**
  - Monitora serviços de proteção endpoint da Symantec em máquinas com Symantec Endpoint Protection. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Trend Micro Client Server Security Services - {Severity3}**
  - Monitora serviços de segurança de servidor cliente da Trend Micro em máquinas com Trend Micro Client Server Security. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Trend Micro OfficeScan Services - {Severity3}**
  - Monitora serviços Trend Micro OfficeScan em máquinas com Trend Micro OfficeScan. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Sistemas Web

- **Web Systems - FTP Server Service - {Severity3}**
  - Monitora o serviço do servidor FTP em servidores FTP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Web Systems - IIS Performance - {Severity3}**
  - Monitora o desempenho de IIS em servidores IIS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Web Systems - IIS Server - {Severity0}**
  - Coleta contadores de desempenho de servidor IIS em servidores IIS. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Web Systems - IIS Server Services - {Severity3}**
  - Monitora serviços de servidor IIS em servidores IIS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Web Systems - SharePoint Server Services - {Severity3}**
  - Monitora serviços de servidor SharePoint em servidores SharePoint. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Conjunto de eventos

Uma variedade de conjuntos de eventos são fornecidos e aplicados através de políticas relacionadas a monitoramento. Esses conjuntos de eventos monitoram logs de eventos do Windows quanto a eventos específicos. Os conjuntos de eventos fornecidos incluem monitoramento de eventos de SO Windows importantes para sistemas Microsoft comuns, como Active Directory, Exchange, SQL, IIS, para sistemas/aplicativos de terceiros e muito mais. Os conjuntos de eventos incluídos são descritos abaixo, agrupados por categoria.

Nesta seção

Segurança

- **zz[SYS] AV - McAfee Anti-Virus (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do McAfee Anti-Virus no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] AV - Microsoft SE-FEP (EW) - SYS - {Severity2}**
  - Monitora eventos de erro e aviso específicos do Microsoft Security Essentials/Forefront Endpoint Protection no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] AV - Misc AntiVirus (EW) - APP-SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de antivírus geral nos logs de eventos de aplicativos e sistemas. Os alarmes são considerados de gravidade 3.
- **zz[SYS] AV - Misc AntiVirus (I) - APP-SYS - {Severity1}**
  - Monitora eventos informativos específicos de antivírus geral nos logs de eventos de aplicativos e sistemas. Os alarmes são considerados de gravidade 1.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Symantec/Norton AntiVirus no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Symantec/Norton AntiVirus no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Symantec/Norton AntiVirus no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] AV - Symantec/Norton AntiVirus (I) - APP - {Severity0}**
  - Monitora eventos específicos informativos do Symantec/Norton AntiVirus no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.

Backup

- zz[SYS] Backup - Backup Exec (EW) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso de execução de backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Backup - Backup Exec (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso de execução de backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Backup - Backup Exec (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso de execução de backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Backup - Backup Exec (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso de execução de backup no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- zz[SYS] Backup - Backup Exec (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de execução de backup no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Backup - Backup Exec Job Failure/Cancellation (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso de cancelamento/falha de execução de backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Backup - Backup Exec Job Success (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de êxito de trabalho na execução de backup no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Backup - BrightStor ARCserve (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do BrightStor ARCserve no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Backup - BrightStor ARCServe (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso do BrightStor ARCServe no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- zz[SYS] Backup - Microsoft Windows Backup (E) - APP - {Severity2}
  - Monitora eventos específicos de erro de backup do Microsoft Windows no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Backup - Misc Backup (E) - APP - {Severity1}
  - Monitora eventos específicos de erro de backup geral no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Backup - Misc Backup (I) - APP - {Severity0}
  - Monitora eventos específicos informativos de backup geral no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Backup - Misc Backup (W) - APP - {Severity1}
  - Monitora eventos específicos de avisos de backup geral no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.

Banco de dados

- zz[SYS] Database - SQL Server (E) - APP - {Severity2}
  - Monitora eventos específicos de erro de SQL Server no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server (E) - APP - {Severity3}

- Monitora eventos específicos de erro de SQL Server no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso do SQL Server - ACID no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - ACID no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do SQL Server - ACID no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - ACID (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de erro de SQL Server - ACID no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do SQL Server - backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - Backup (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de erro de SQL Server - backup no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso do SQL Server - recursos de banco de dados no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - recursos de banco de dados no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do SQL Server - recursos de banco de dados no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - DB Resources (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de erro de SQL Server - recursos de banco de dados no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso do SQL Server - MSDTC no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - MSDTC no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do SQL Server - MSDTC no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - MSDTC (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de erro de SQL Server - MSDTC no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.

- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do SQL Server - rede no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do SQL Server - rede no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do SQL Server - consulta no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do SQL Server - consulta no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do SQL Server - replicação no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do SQL Server - replicação no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do SQL Server - replicação no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Database - SQL Server - Replication (EWISFCV) - APP - {Severity0}**
  - Monitora eventos específicos de erro de SQL Server - replicação no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do SQL Server - geração de relatórios no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do SQL Server - geração de relatórios no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Database - SQL Server - Reporting (EWISFCV) - APP - {Severity0}**
  - Monitora eventos específicos de erro de SQL Server - geração de relatórios no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do agente SQL Server - várias instâncias no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do agente SQL Server - várias instâncias no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do agente SQL Server - várias instâncias no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EWISFCV) - APP - {Severity0}**
  - Monitora eventos específicos de erro do agente SQL Server - várias instâncias no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity1}**

- Monitora eventos específicos de erro e aviso do agente SQL Server - instância única no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.

- zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do agente SQL Server - instância única no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do agente SQL Server - instância única no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server Agent - Single Instance (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de erro do agente SQL Server - instância única no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Database - SQL Server Cluster (I) - SYS - {Severity2}
  - Monitora eventos específicos informativos de cluster do SQL Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL/Service Control Manager (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso do gerenciador de controle do SQL Server no log de eventos do sistema. Os alarmes são considerados de gravidade 3.

E-mail

- zz[SYS] Email - Blackberry Server (E) - APP - {Severity1}
  - Monitora eventos específicos de erro de servidor Blackberry no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Email - Blackberry Server (W) - APP - {Severity1}
  - Monitora eventos específicos de aviso de servidor Blackberry no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Email - Blackberry Server (W) - APP - {Severity2}
  - Monitora eventos específicos de aviso de servidor Blackberry no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Email - Blackberry Server Events (E) - APP - {Severity3}
  - Monitora eventos específicos de erro de eventos de servidor Blackberry no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Email - Blackberry Server Events (W) - APP - {Severity2}
  - Monitora eventos específicos de aviso de eventos de servidor Blackberry no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Email - Exchange 2000 and 2003 (E) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso do Exchange 2000 e 2003 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do Exchange 2000 e 2003 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do Exchange 2000 e 2003 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Email - Exchange 2000 and 2003 and 2007 (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do Exchange 2000, 2003 e 2007 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity1}

- Monitora eventos específicos de erro e aviso do Exchange 2007 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.

- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 (EWISFCV) - APP - {Severity0}**
  - Monitora eventos específicos de execução do Exchange 2007 no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Acesso a cliente no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Acesso a cliente no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Acesso a cliente no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de borda no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de borda no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de borda no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de hub no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de hub no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de hub no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Caixa de correio no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Caixa de correio no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Caixa de correio no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EWISFCV) - APP - {Severity0}**

- Monitora eventos específicos de execução do Exchange 2007 - Caixa de correio no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.

- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Serviços de transporte no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Serviços de transporte no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Serviços de transporte no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Sistema de mensagens unificadas no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Sistema de mensagens unificadas no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Sistema de mensagens unificadas no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2010 Server (E) - APP - {Severity1}**
  - Monitora eventos específicos de erro de servidor Exchange 2010 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso de servidor Exchange 2010 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso de servidor Exchange 2010 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso de servidor Exchange 2010 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity2}**
  - Monitora eventos específicos de erro de servidor Exchange no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity3}**
  - Monitora eventos específicos de erro de servidor Exchange no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange Server (I) - SYS - {Severity3}**
  - Monitora eventos específicos informativos de servidor Exchange no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange Server 5.5 (E) - APP - {Severity3}**
  - Monitora eventos específicos de erro de servidor Exchange 5.5 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange/Service Control Manager (EW) - SYS - {Severity3}**

- Monitora eventos específicos de erro e aviso do gerenciador de controle de serviço/Exchange no log de eventos do sistema. Os alarmes são considerados de gravidade 3.

- **zz[SYS] Email - SMTP/Service Control Manager (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso do gerenciador de controle de serviço/SMTP no log de eventos do sistema. Os alarmes são considerados de gravidade 3.

Hardware

- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de bateria Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de bateria Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de bateria Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Battery (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de bateria Dell no registro de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de controlador Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de controlador Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de controlador Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Controller (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de controlador Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de aviso e erro elétrico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de aviso e erro elétrico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de aviso e erro elétrico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Electrical (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos elétricos Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de carcaça Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity2}**

- Monitora eventos específicos de erro e aviso de carcaça Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.

- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de carcaça Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Enclosure (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de carcaça Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso ambientais Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso ambientais Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso ambientais Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Environmental (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos ambientais Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de ventoinha Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de ventoinha Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de ventoinha Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Fan (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de ventoinha Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de alterações de hardware Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de alterações de hardware Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de alterações de hardware Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Hardware Changes (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de alterações ambientais Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de log de hardware Dell no log de eventos de sistemas. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity2}**

- ➢ Monitora eventos específicos de erro e aviso de log de hardware Dell no log de eventos de sistemas. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Hardware Log (EWISFCV) - SYS - {Severity0}**
  - ➢ Monitora eventos específicos de log de hardware Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity1}**
  - ➢ Monitora eventos específicos de erro e aviso de mídia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity2}**
  - ➢ Monitora eventos específicos de erro e aviso de mídia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity3}**
  - ➢ Monitora eventos específicos de erro e aviso de mídia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Media (EWISFCV) - SYS - {Severity0}**
  - ➢ Monitora eventos específicos de mídia Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity1}**
  - ➢ Monitora eventos específicos de erro e aviso pré-falha de memória Dell no log de eventos de sistemas. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity2}**
  - ➢ Monitora eventos específicos de erro e aviso pré-falha de memória Dell no log de eventos de sistemas. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity1}**
  - ➢ Monitora eventos específicos de erro e aviso de sistema OMSA Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity2}**
  - ➢ Monitora eventos específicos de erro e aviso de sistema OMSA Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity3}**
  - ➢ Monitora eventos específicos de erro e aviso de sistema OMSA Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell OMSA System (EWISFCV) - SYS - {Severity0}**
  - ➢ Monitora eventos específicos de sistema OMSA Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity2}**
  - ➢ Monitora eventos específicos de erro e aviso de sistema OMSM Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity3}**
  - ➢ Monitora eventos específicos de erro e aviso de sistema OMSM Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity1}**
  - ➢ Monitora eventos específicos de erro e aviso de disco físico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity2}**
  - ➢ Monitora eventos específicos de erro e aviso de disco físico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity3}**

- Monitora eventos específicos de erro e aviso de disco físico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Physical Disk (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de disco físico Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de gestão de energia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de gestão de energia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de gestão de energia Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Power Management (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de gestão de energia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 0.
- **zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de processador Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de processador Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Processor (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de processador Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de espelho de redundância Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de espelho de redundância Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Redundancy Mirror (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de espelho de redundância Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de temperatura Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de temperatura Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de temperatura Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Temperature (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de temperatura Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity1}**

- Monitora eventos específicos de erro e aviso de disco virtual Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso de disco virtual Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - Dell Virtual Disk (EWISFCV) - SYS - {Severity0}
  - Monitora eventos específicos de disco virtual Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Hardware - HP Top Tools (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso de principais ferramentas HP no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - HP/Compaq Insight Manager (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso de HP/Compaq Insight Manager no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - HP/Compaq StorageWorks (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso de HP/Compaq StorageWorks no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - IBM SeriesX Events (E) - APP - {Severity2}
  - Monitora eventos específicos de erro de eventos de IBM SeriesX no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Hardware - Misc HW (E) - SYS - {Severity1}
  - Monitora eventos específicos de erro de hardware geral no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Hardware - Misc HW (E) - SYS - {Severity2}
  - Monitora eventos específicos de erro de hardware geral no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- zz[SYS] Hardware - Misc HW (W) - SYS - {Severity1}
  - Monitora eventos específicos de aviso de hardware geral no log de eventos do sistema. Os alarmes são considerados de gravidade 1.

Infraestrutura de rede

- zz[SYS] Network Infrastructure - Active Directory (E) - SYS - {Severity1}
  - Monitora eventos específicos de erro de Active Directory no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity1}
  - Monitora eventos específicos de aviso de Active Directory no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity2}
  - Monitora eventos específicos de aviso de Active Directory no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- zz[SYS] Network Infrastructure - Active Directory Events (E) - APP - {Severity3}
  - Monitora eventos específicos de erro de eventos de Active Directory no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Network Infrastructure - Active Directory Events (W) - APP - {Severity2}
  - Monitora eventos específicos de aviso de eventos de Active Directory no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Network Infrastructure - Active Directory Logon/Logoff/Lockout Activity (F) - SEC - {Severity3}

- Monitora eventos específicos de auditoria de falha de atividade de logon/logoff/bloqueio do Active Directory no log de eventos de segurança. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erro NTDS de Active Directory no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity3}**
  - Monitora eventos específicos de erro NTDS de Active Directory no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (I) - SYS - {Severity0}**
  - Monitora eventos específicos informativos de NTDS de Active Directory no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Network Infrastructure - DHCP Server (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erro de servidor DHCP no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - DHCP Server (W) - SYS - {Severity1}**
  - Monitora eventos específicos de aviso de servidor DHCP no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - DNS Server (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erro de servidor DNS no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - DNS Server (W) - SYS - {Severity1}**
  - Monitora eventos específicos de aviso de servidor DNS no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - WINS Server (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erro de servidor WINS no log de eventos do sistema. Os alarmes são considerados de gravidade 1.

Acesso remoto

- **zz[SYS] Remote Access - Citrix MetaFrame (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Citrix MetaFrame no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Remote Access - Citrix Server Events (E) - APP - {Severity2}**
  - Monitora eventos específicos de erro de eventos de servidor Citrix no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity2}**
  - Monitora eventos específicos de erro de eventos de servidor Terminal no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity3}**
  - Monitora eventos específicos de erro de eventos de servidor Terminal no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.

Sistemas Web

- **zz[SYS] Web Systems - IIS 6 Events (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso de eventos do IIS 6 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity2}**

- Monitora eventos específicos de erro de eventos do IIS 7 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.

- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity3}**
  - Monitora eventos específicos de erro de eventos do IIS 7 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Web Systems - IIS Server (E) - APP - {Severity1}**
  - Monitora eventos específicos de erro de servidor IIS no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Web Systems - IIS Server (W) - APP - {Severity1}**
  - Monitora eventos específicos de aviso de servidor IIS no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.

Plataformas de SO

- **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity2}**
  - Monitora eventos específicos de erros comuns do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity3}**
  - Monitora eventos específicos de erros comuns do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server (Core) Events (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos comuns do Windows Server no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity1}**
  - Monitora eventos específicos comuns de auditoria com falha do Windows Server no log de eventos de segurança. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity3}**
  - Monitora eventos específicos comuns de auditoria com falha do Windows Server no log de eventos de segurança. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity1}**
  - Monitora eventos específicos comuns de aviso do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity2}**
  - Monitora eventos específicos comuns de aviso do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server (Core) Ignore Events - (EW) - APP-SYS - {Ignore}**
  - Ignora o monitoramento de eventos específicos de avisos e erros comuns do Windows Server no log de eventos de aplicativos e sistemas.
- **zz[SYS] OS - Windows Server (Core) Printer Spooler (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de spooler de impressão do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso do gerenciador de controle de serviço do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso do gerenciador de controle de serviço do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 3.

- **zz[SYS] OS - Windows Server (Core) Service Control Manager (I) - SYS - {Severity2}**
  - Monitora eventos específicos informativos do gerenciador de controle de serviço do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server (Core) System Shutdown (W) - SYS - {Severity2}**
  - Monitora eventos específicos de aviso de desligamento do sistema do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erros comuns do Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity3}**
  - Monitora eventos específicos de erros comuns do Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server 2008 (Core) Events (W) - SYS - {Severity1}**
  - Monitora eventos específicos comuns de aviso do Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Advanced Windows Server 2008 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Advanced Windows Server 2008 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Advanced Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Advanced Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Advanced Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server 2008 Advanced (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos comuns do Advanced Windows Server 2008 no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Basic Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Basic Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Basic Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server 2008 Basic (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos comuns do Basic Windows Server 2008 no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity1}**

- Monitora eventos específicos comuns de auditoria com falha do Basic Windows Server 2008 no log de eventos de segurança. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity2}**
  - Monitora eventos específicos comuns de auditoria com falha do Basic Windows Server 2008 no log de eventos de segurança. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity3}**
  - Monitora eventos específicos comuns de auditoria com falha do Basic Windows Server 2008 no log de eventos de segurança. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Workstation (Core) Events (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erros comuns de estação de trabalho com Windows no log de eventos do sistema. Os alarmes são considerados de gravidade 1.

Capítulo 4

Catálogo de conteúdo completo

Os tópicos a seguir resumem a lista completa de todo o conteúdo padrão fornecido com o VSA.

Neste capítulo

Vistas

Status do agente

- zz[SYS] Agent - Has Checked In
  - Exibe todas as máquinas que entraram pelo menos uma vez (exclui Modelos).
- zz[SYS] Agent - Has Not Checked In
  - Exibe todos os agentes que não entraram (ou seja, modelos e computadores de implementação KDS).
- zz[SYS] Agent - Offline
  - Exibe todos os agentes off-line por mais de um minuto.
- zz[SYS] Agent - Offline 30+ Days
  - Exibe todos os agentes off-line por mais de 30 dias.
- zz[SYS] Agent - Offline 60+ Days
  - Exibe todos os agentes off-line por mais de 60 dias.
- zz[SYS] Agent - Online
  - Exibe todos os agentes on-line no último minuto.
- zz[SYS] Agent - Online in Last 30 Days
  - Exibe todos os agentes on-line nos últimos 7 dias.
- zz[SYS] Agent - Rebooted 14+ Days Ago
  - Exibe todos os agentes que NÃO foram reinicializados nos últimos 14 dias.
- zz[SYS] Agent - Suspended
  - Exibe todos os agentes suspensos.
- zz[SYS] Agent - User Logged On
  - Exibe todas as máquinas com um usuário conectado nelas.

Segurança

- zz[SYS] AV - AVG Technologies
  - Exibe todas as máquinas com Grisoft AVG Anti-Virus instalado.
- zz[SYS] AV - Kaspersky ES
  - Exibe todas as máquinas com o Kaspersky Endpoint Security instalado.
- zz[SYS] AV - McAfee
  - Exibe todas as máquinas com McAfee Anti-Virus instalado.
- zz[SYS] AV - Microsoft SE-FEP
  - Exibe todas as máquinas com Microsoft Security Essentials ou Forefront Endpoint Protection instalado.
- zz[SYS] AV - Sophos
  - Exibe todas as máquinas com Sophos Anti-Virus instalado.
- zz[SYS] AV - Symantec AV
  - Exibe todas as máquinas com Symantec Anti-Virus instalado.
- zz[SYS] AV - Symantec EP
  - Exibe todas as máquinas com Symantec Endpoint Protection instalado.
- zz[SYS] AV - Trend Micro
  - Exibe todas as máquinas com Trend Micro Anti-Virus instalado.

Backup

- **zz[SYS] Backup - CA BrightStor ARCServe**
  - Exibe todas as máquinas com o CA BrightStor ARCserve instalado.
- **zz[SYS] Backup - Symantec Backup Exec**
  - Exibe todas as máquinas com Symantec Backup Exec instalado.

Hardware

- **zz[SYS] HW - Apple**
  - Exibe todas as máquinas com Apple como fabricante.
- **zz[SYS] HW - Dell**
  - Exibe todas as máquinas com Dell como fabricante.
- **zz[SYS] HW - Dell PowerEdge**
  - Exibe todas as máquinas com Dell como fabricante e PowerEdge no nome do produto.
- **zz[SYS] HW - HP**
  - Exibe todas as máquinas com HP ou Hewlett Packard como fabricante.
- **zz[SYS] HW - HP ProLiant**
  - Exibe todas as máquinas com HP ou Hewlett Packard como fabricante e ProLiant no nome do produto.
- **zz[SYS] HW - IBM**
  - Exibe todas as máquinas com IBM como fabricante.
- **zz[SYS] HW - IBM Series X**
  - Exibe todas as máquinas com IBM como fabricante e Series X no nome do produto.
- **zz[SYS] HW - Lenovo**
  - Exibe todas as máquinas com Lenovo como fabricante.
- **zz[SYS] HW - Not Portable**
  - Exibe todas as máquinas que não são móveis.
- **zz[SYS] HW - Portable**
  - Exibe todas as máquinas que são móveis (ou seja, tipo de chassi = notebook ou laptop; portátil ou tablet pc; portátil ou subnotebook, ou netbook). Nota: Máquinas Mac OS X e Linux não estão incluídas.
- **zz[SYS] HW - Under 1GB Memory**
  - Exibe todas as máquinas que tenham menos de 1 GB de memória.
- **zz[SYS] HW - Under 512MB Memory**
  - Exibe todas as máquinas que tenham menos de 512 MB de memória.
- **zz[SYS] HW - Virtual Guest**
  - Exibe todas as máquinas que são computadores virtualizados (guests VMware, XenServer, VirtualBox ou HyperV).

Rede

- **zz[SYS] Network - 10.11.12.x**
  - Exibe todos os agentes de sub-rede 10.11.12.x de rede específica.

Sistema operacional

- **zz[SYS] OS - All Linux**
  - Exibe todas as máquinas Linux.
- **zz[SYS] OS - All Mac OS X**
  - Exibe todas as máquinas Mac OS X.

- **zz[SYS] OS - All Mac OS X Servers**
  - Exibe todas as máquinas Mac OS X Server.
- **zz[SYS] OS - All Mac OS X Workstations**
  - Exibe todas as máquinas Mac OS X Workstation.
- **zz[SYS] OS - All Servers**
  - Exibe todas as máquinas executando um sistema operacional de classe de servidor.
- **zz[SYS] OS - All Windows**
  - Exibe todas as máquinas com Windows.
- **zz[SYS] OS - All Windows SBS**
  - Exibe todas as máquinas com Windows SBS Server.
- **zz[SYS] OS - All Windows Servers**
  - Exibe todas as máquinas com Windows Server.
- **zz[SYS] OS - All Windows Workstations**
  - Exibe todas as máquinas com Windows Workstation.
- **zz[SYS] OS - All Workstations**
  - Exibe todas as máquinas executando um sistema operacional de classe de estação de trabalho.
- **zz[SYS] OS - Mac OS X 10.5 Leopard**
  - Exibe todas as máquinas com Mac OS X 10.5.
- **zz[SYS] OS - Mac OS X 10.6 Snow Leopard**
  - Exibe todas as máquinas com Mac OS X 10.6.
- **zz[SYS] OS - Mac OS X 10.7 Lion**
  - Exibe todas as máquinas com Mac OS X 10.7.
- **zz[SYS] OS - Mac OS X 10.8 Mountain Lion**
  - Exibe todas as máquinas com Mac OS X 10.8.
- **zz[SYS] OS - Win 2003 SBS**
  - Exibe todas as máquinas executando um sistema operacional Windows 2003 Small Business Server.
- **zz[SYS] OS - Win 2003 Server**
  - Exibe todas as máquinas executando um sistema operacional Windows 2003 Server.
- **zz[SYS] OS - Win 2008 R2 Server**
  - Exibe todas as máquinas executando um sistema operacional Windows 2008 Small Business Server.
- **zz[SYS] OS - Win 2008 SBS**
  - Exibe todas as máquinas executando um sistema operacional Windows 2008 Server.
- **zz[SYS] OS - Win 2008 Server**
  - Exibe todas as máquinas executando um sistema operacional Windows 2008 Server R2.
- **zz[SYS] OS - Win 2012 Server**
  - Exibe todas as máquinas executando um sistema operacional Windows 2012 Server.
- **zz[SYS] OS - Win 7**
  - Exibe todas as máquinas executando um sistema operacional Windows 7.
- **zz[SYS] OS - Win Vista**
  - Exibe todas as máquinas executando um sistema operacional Windows Vista.
- **zz[SYS] OS - Win XP**
  - Exibe todas as máquinas executando um sistema operacional Windows XP.

- **zz[SYS] OS - Win 8**
  - Exibe todas as máquinas executando um sistema operacional Windows 8.

Gerenciamento da correção

- **zz[SYS] Patch - Deny Patching Policy**
  - Exibe todas as máquinas que estão na política de correções "Recusar correções".
- **zz[SYS] Patch - Missing 10+ Approved Patches**
  - Exibe todas as máquinas que estão com 10 ou mais correções aprovadas ausentes com base em suas participações de política de correções.
- **zz[SYS] Patch - Missing 20+ Approved Patches**
  - Exibe todas as máquinas que estão com 20 ou mais correções aprovadas ausentes com base em suas participações de política de correções.
- **zz[SYS] Patch - No Policy**
  - Exibe todas as máquinas que não são membro de uma Política de correções.
- **zz[SYS] Patch - Pending Reboot**
  - Exibe todas as máquinas que estão com reinicialização pendente devido a atualizações de correções recentes.
- **zz[SYS] Patch - Scan Failed**
  - Exibe todas as máquinas que falharam na verificação de correções.
- **zz[SYS] Patch - Scan Not Scheduled**
  - Exibe todas as máquinas que não tiveram uma varredura de correção agendada.
- **zz[SYS] Patch - Server Patching Policy**
  - Exibe todas as máquinas que estão na política de correções "Correções de servidor".
- **zz[SYS] Patch - Servers w No Policy**
  - Exibe todas as máquinas que não são membro de uma Política de correções.
- **zz[SYS] Patch - Test Patching Group**
  - Exibe todas as máquinas que foram designadas como sistemas de testes para gerenciamento de correções.
- **zz[SYS] Patch - Windows Auto Update Enabled**
  - Exibe todas as máquinas com atualização automática do Windows ativada.
- **zz[SYS] Patch - Workstation Patching Policy**
  - Exibe todas as máquinas que estão na política de correções "Correções de estação de trabalho".
- **zz[SYS] Patch - Workstations w No Policy**
  - Exibe todas as máquinas que não são membro de uma Política de correções.

Função de servidor

- **zz[SYS] Role - Backup Exec Server**
  - Exibe todos os servidores de execução de backup.
- **zz[SYS] Role - Blackberry Server**
  - Exibe todos os servidores Blackberry Enterprise.
- **zz[SYS] Role - Brightstor ARCserve Server**
  - Exibe todos os servidores BrightStor ARCserve.
- **zz[SYS] Role - Citrix Server**
  - Exibe todos os servidores Citrix.
- **zz[SYS] Role - DHCP Server**
  - Exibe todos os servidores MS DHCP.

- **zz[SYS] Role - DNS Server**
  - Exibe todos os servidores MS DNS.
- **zz[SYS] Role - Domain Controller**
  - Exibe todos os servidores MS AD Domain Controller.
- **zz[SYS] Role - Exchange 2003 Server**
  - Exibe todos os servidores MS Exchange 2003.
- **zz[SYS] Role - Exchange 2007 Server**
  - Exibe todos os servidores MS Exchange 2007.
- **zz[SYS] Role - Exchange 2010 Server**
  - Exibe todos os servidores MS Exchange 2010.
- **zz[SYS] Role - Exchange Server**
  - Exibe todos os servidores MS Exchange.
- **zz[SYS] Role - File Server**
  - Exibe todos os servidores de arquivo MS.
- **zz[SYS] Role - FTP Server**
  - Exibe todos os servidores MS FTP.
- **zz[SYS] Role - IIS Server**
  - Exibe todos os servidores MS IIS.
- **zz[SYS] Role - IMAP4 Server**
  - Exibe todos os servidores MS Exchange IMAP4.
- **zz[SYS] Role - POP3 Server**
  - Exibe todos os servidores MS Exchange POP3.
- **zz[SYS] Role - Print Server**
  - Exibe todos os servidores de impressão MS.
- **zz[SYS] Role - SharePoint Server**
  - Exibe todos os servidores MS SharePoint.
- **zz[SYS] Role - SMTP Server**
  - Exibe todos os servidores MS SMTP.
- **zz[SYS] Role - SQL Server**
  - Exibe todos os servidores MS SQL.
- **zz[SYS] Role - SQL Server 2005**
  - Exibe todos os servidores MS SQL 2005.
- **zz[SYS] Role - SQL Server 2008**
  - Exibe todos os servidores MS SQL 2008.
- **zz[SYS] Role - Terminal Server**
  - Exibe todos os servidores MS Terminal em Modo aplicativo.
- **zz[SYS] Role - WINS Server**
  - Exibe todos os servidores MS WINS.

Políticas

[System].Core.Global Policies.Agent Settings

- **Agente (Core)**
  - *Modo de visualização da política:* zz[SYS] Policy - Agent_Has Checked In

- *Descrição:* Agente (Core): aplica configurações comuns do agente para todas as máquinas gerenciadas. O ícone de agente está ativo, somente a opção Atualizar está ativada. O controle de entrada está definido como 30 segundos com as opções "Avisar se houver vários agentes usando a mesma conta" e "Avisar se o agente na mesma LAN que o KServer se conectar através do gateway" ativadas. O histórico de logs do agente para todos os logs está definido como 31 dias.

- **Agente Windows**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows
  - *Descrição:* Agente Windows: aplica configurações do agente específicas para Windows. Define o diretório de trabalho do agente como c:\kworking.
- **Agente Linux**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Linux
  - *Descrição:* Agente Linux: aplica configurações do agente específicas para Linux. Define o diretório de trabalho do agente como /tmp/kworking.
- **Agente Macintosh**
  - *Modo de visualização da política:*zz[SYS] Policy - OS_All Mac OS X
  - *Descrição:* Agente Macintosh: aplica configurações do agente específicas para Macintosh Workstations. Define o diretório de trabalho do agente como /Library/Kaseya/kworking.

[System].Core.Global Policies.Remote Support

- **Server RC Notification Policy (Silent w Admin Note)**
  - *Modo de visualização da política:*zz[SYS] Policy - OS_All Servers
  - *Descrição:* Política de notificação de CR de servidor (silencioso com ação de admin.): aplica a configuração de notificação de CR a todos os servidores. Define o tipo de notificação de usuário como Assumir controle silenciosamente; além disso, ativa a opção Requer a ação do admin para iniciar o controle remoto.
- **Workstation RC Notification Policy (Alert/Term w Admin Note)**
  - *Modo de visualização da política:*zz[SYS] Policy - OS_All Workstations
  - *Descrição:* Política de notificação de CR de estação de trabalho (alerta/termo com ação de admin): aplica configurações de notificação de CR a todas as estações de trabalho. Define o tipo de notificação de usuário como Se o usuário estiver conectado exibir um alerta, Notificar o usuário quando a sessão terminar e ativa a opção Requer a ação do admin. para iniciar o controle remoto.

[System].Core.Org Specific Policies.Agent Settings

- **Agente (Oculto)**
  - *Modo de visualização da política:*zz[SYS] Policy - Agent_Has Checked In
  - *Descrição:* Agente (Oculto): aplica configurações comuns do agente para todas as máquinas gerenciadas. O ícone do agente está desativado/oculto. O controle de entrada está definido como 30 segundos com as opções "Avisar se houver vários agentes usando a mesma conta" e "Avisar se o agente na mesma LAN que o KServer se conectar através do gateway" ativadas. O histórico de logs do agente para todos os logs está definido como 31 dias.
- **Agente (Servidor)**
  - *Modo de visualização da política:*zz[SYS] Policy - OS_All Servers
  - *Descrição:* Agente (Servidor): aplica configurações comuns do agente a todos os servidores gerenciados. O ícone do agente está ativado com Desativar controle remoto, Atualizar e Sair. O controle de entrada está definido como 30 segundos com as opções "Avisar se houver vários agentes usando a mesma conta" e "Avisar se o agente na mesma

LAN que o KServer se conectar através do gateway" ativadas. O histórico de logs do agente para todos os logs está definido como 93 dias.

- **Agente (Estação de trabalho)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Workstations
  - *Descrição:* Agente (Estação de trabalho): aplica configurações comuns do agente a todas as estações de trabalho gerenciadas. O ícone do agente está ativado com Contato com Help Desk, Desativar controle remoto e Atualizar. O controle de entrada está definido como 30 segundos com as opções "Avisar se houver vários agentes usando a mesma conta" e "Avisar se o agente na mesma LAN que o KServer se conectar através do gateway" ativadas. O histórico de logs do agente para todos os logs está definido como 31 dias.

[System].Core.Org Specific Policies.Remote Support

- **Server RC Notification Policy (Silent w/o Admin Note)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Servers
  - *Descrição:* Política de notificação de CR de servidor (silencioso sem ação de admin.): aplica a configuração de notificação de CR a todos os servidores. Define o tipo de notificação de usuário como Assumir controle silenciosamente e não requer ação do admin. para iniciar o controle remoto.
- **Workstation RC Notification Policy (Alert/Term w/o Admin Note)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Workstations
  - *Descrição:* Política de notificação de CR de estação de trabalho (alerta/termo sem ação de admin.): aplica configurações de notificação de CR a todas as estações de trabalho. Define o tipo de notificação de usuário como Se o usuário estiver conectado exibir um alerta, Notificar o usuário quando a sessão terminar e não requer a ação do admin. para iniciar o controle remoto.
- **Workstation RC Notification Policy (Silent w Admin Note)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Workstations
  - *Descrição:* Política de notificação de CR de estação de trabalho (silencioso com ação de admin.): aplica a configuração de notificação de CR a todas as estações de trabalho. Define o tipo de notificação de usuário como Assumir controle silenciosamente, mas requer ação do admin. para iniciar o controle remoto.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Baseline.Baseline Audit Schedule (Annually Daytime)

- **Baseline Audit Schedule (Annually Jan 1-7 6am-6pm/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Agent_Has Checked In
  - *Descrição:* Agendamento de auditoria da linha de base (anualmente, de 1º a 7 de janeiro, das 6h às 18h/gestão de energia): aplica uma auditoria de linha de base anual agendada para todas as máquinas que foram implantadas e iniciadas, de 1º de janeiro a 7 de janeiro, entre 6h e 18h. A política usa o recurso de gestão de energia no horário de auditoria agendado, tentando ativar uma máquina desligada antes da auditoria. A política é geralmente usada em situações em que auditorias anuais podem ser necessárias para fins de planejamento ou conformidade; comparações de auditoria de linha de base/mais recentes relevantes também podem ser realizadas para tarefas operacionais. A política pode ser seletivamente aplicada a várias máquinas, grupos de máquinas e/ou organizações inteiras de máquinas.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Daytime)

- **Latest/SysInfo Audit Schedule (Daily M-F 6am-6pm/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Agent_Has Checked In

- *Descrição:* Agendamento de auditoria mais recente/SysInfo (diariamente, de segunda a sexta, das 6h às 18h/gestão de energia): aplica auditorias de informações do sistema e mais recentes agendadas a todas as máquinas que entraram em execução diariamente (de segunda a sexta), das 6h às 18h. A política usa o recurso de gestão de energia no horário de auditoria agendado, tentando ativar uma máquina desligada antes da auditoria. Em geral, a política é usada em situações nas quais clientes precisam realizar auditorias durante o horário comercial em dias de semana, pois as máquinas geralmente estão desligadas à noite e em finais de semana. A política pode ser seletivamente aplicada a várias máquinas, grupos de máquinas e/ou organizações inteiras de máquinas.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Daily.Latest/SysInfo Audit Schedule (Daily Nighttime)

- **Latest/SysInfo Audit Schedule (Daily M-F 6pm-6am/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Agent_Has Checked In
  - *Descrição:* Agendamento de auditoria mais recente/SysInfo (diariamente, de segunda a sexta, das 18h às 6h/gestão de energia): aplica auditorias de informações do sistema e mais recentes agendadas a todas as máquinas que entraram em execução diariamente (de segunda a sexta), das 18h às 6h. A política usa o recurso de gestão de energia no horário de auditoria agendado, tentando ativar uma máquina desligada antes da auditoria. A política em geral é usada em situações nas quais clientes preferem realizar auditorias durante o turno da noite quando sistemas são menos utilizados do que no horário comercial, bem como quando máquinas são deixadas ligadas à noite ou foram configuradas Wake-On-LAN ou vPro Power Management para que possam ser ativadas se forem desligadas à noite. A política pode ser seletivamente aplicada a várias máquinas, grupos de máquinas e/ou organizações inteiras de máquinas.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Weekly.Latest/SysInfo Audit Schedule (Weekly Daytime)

- **Latest/SysInfo Audit Schedule (Weekly M-F 6am-6pm/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Agent_Has Checked In
  - *Descrição:* Agendamento de auditoria mais recente/SysInfo (semanalmente, de segunda a sexta, das 6h às 18h/gestão de energia): aplica auditorias de informações do sistema e mais recentes agendadas a todas as máquinas que entraram em execução semanalmente (de segunda a sexta), das 6h às 18h. A política usa o recurso de gestão de energia no horário de auditoria agendado, tentando ativar uma máquina desligada antes da auditoria. Em geral, a política é usada em situações nas quais clientes precisam realizar auditorias durante o horário comercial em dias de semana, pois as máquinas geralmente estão desligadas à noite e em finais de semana. A política pode ser seletivamente aplicada a várias máquinas, grupos de máquinas e/ou organizações inteiras de máquinas.

[System].Core.Org Specific Policies.Audit / Inventory.Schedules.Latest/SysInfo.Weekly.Latest/SysInfo Audit Schedule (Weekly Nighttime)

- **Latest/SysInfo Audit Schedule (Weekly M-F 6pm-6am/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Agent_Has Checked In
  - *Descrição:* Agendamento de auditoria mais recente/SysInfo (semanalmente, de segunda a sexta, das 18h às 6h/gestão de energia): aplica auditorias de informações do sistema e mais recentes agendadas a todas as máquinas que entraram em execução semanalmente (de segunda a sexta), das 18h às 6h. A política usa o recurso de gestão de energia no horário de auditoria agendado, tentando ativar uma máquina desligada antes da auditoria. A política em geral é usada em situações nas quais clientes preferem realizar auditorias durante o turno da noite quando sistemas são menos utilizados do que no horário comercial, bem como quando máquinas são deixadas ligadas à noite ou foram configuradas Wake-On-LAN ou vPro Power Management para que possam ser ativadas se forem

desligadas à noite. A política pode ser seletivamente aplicada a várias máquinas, grupos de máquinas e/ou organizações inteiras de máquinas.

[System].Core.Org Specific Policies.Maintenance.Windows Workstation Recurring Maintenance

- **Windows Workstation Maintenance (Weekly M-F 6pm-6am)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows Workstations
  - *Descrição:* Manutenção de estação de trabalho Windows (semanalmente, de segunda a sexta, das 18h às 6h): aplica um procedimento de manutenção de estação de trabalho Windows agendado para execução a todas as máquinas de estação de trabalho Windows, semanalmente (de segunda a sexta), das 18h às 6h. Se a máquina não estiver ligada quando a manutenção for agendada, então a máquina ignorará esse ciclo de manutenção e tentará executar a manutenção novamente uma semana depois.

[System].Core.Org Specific Policies.Maintenance.Macintosh Workstation Recurring Maintenance

- **Macintosh Maintenance Schedule (Weekly M-F 6pm-6am)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Descrição:* Agendamento de manutenção de Macintosh (semanalmente, de segunda a sexta, das 18h às 6h): aplica um procedimento de manutenção de Macintosh agendado para execução a todas as máquinas Macintosh, semanalmente (de segunda a sexta), das 18h às 6h. Se a máquina não estiver ligada quando a manutenção for agendada, então a máquina ignorará esse ciclo de manutenção e tentará executar a manutenção novamente uma semana depois.

[System].Core.Org Specific Policies.Maintenance.Linux Recurring Maintenance

- **Linux Maintenance Schedule (Weekly M-F 6pm-6am)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Linux
  - *Descrição:* Agendamento de manutenção de Linux (semanalmente, de segunda a sexta, das 18h às 6h): aplica um procedimento de manutenção de Linux agendado para execução a todas as máquinas Linux, semanalmente (de segunda a sexta), das 18h às 6h. Se a máquina não estiver ligada quando a manutenção for agendada, então a máquina ignorará esse ciclo de manutenção e tentará executar a manutenção novamente uma semana depois.

[System].Core.Org Specific Policies.Maintenance.Windows Server Recurring Maintenance

- **Windows Server Maintenance (Weekly Sun 12am-4am)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows Servers
  - *Descrição:* Manutenção de Windows Server (semanalmente, aos domingos, da meia-noite às 4h): aplica um procedimento de manutenção de Windows Server agendado para execução a todas as máquinas Windows Server, semanalmente (aos domingos), da meia-noite às 4h. Se a máquina não estiver ligada quando a manutenção for agendada, então a máquina ignorará esse ciclo de manutenção e tentará executar a manutenção novamente uma semana depois.

[System].Core.Org Specific Policies.Monitoring.Server

- **Server Roles Enhanced Audit**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows Servers
  - *Descrição:* Auditoria aprimorada de funções de servidor: aplica uma auditoria aprimorada agendada para execução semanal, aos domingos, da meia-noite às 4h, para identificar funções de servidor para que políticas de monitoramento possam ser aplicadas devidamente com base nessas funções.
- **Common Windows Server Monitoring**

- *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows Servers
- *Descrição:* Monitoramento comum do Windows Server: aplica um conjunto comum de monitoramento para todos os servidores Windows. Isso inclui log de eventos relacionados a hardware, Windows Service e monitoramento comum de desempenho do Windows.

- **Windows Server (Core)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows Servers
  - *Descrição:* Windows Server (Core): aplica uma variedade de monitoramentos do Windows Server (Core) a Windows Servers, incluindo monitoramento de serviços padrão, desempenho do sistema, geração de relatórios de integridade, logs de eventos e muito mais.
- **Windows Server 2003**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_Win 2003 Server
  - *Descrição:* Windows Server 2003: aplica monitoramento de serviço padrão para Windows 2003 Servers.
- **Windows Server 2008/2008 R2**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_Win 2008 Server
  - *Descrição:* Windows Server 2008/2008 R2: aplica monitoramento de serviço padrão para Windows 2008/2008 R2 Servers.
- **Windows Server 2012**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_Win 2012 Server
  - *Descrição:* Windows Server 2012: aplica monitoramento de serviço padrão para Windows 2012 Servers.

[System].Core.Org Specific Policies.Monitoring.Server.Hardware

- **Dell PowerEdge**
  - *Modo de visualização da política:* zz[SYS] Policy - HW_Dell PowerEdge
  - *Descrição:* Dell PowerEdge: aplica alertas e monitoramento específicos a hardware de servidor Dell PowerEdge. Esse monitoramento pode exigir que ferramentas específicas de monitoramento de servidor Dell PowerEdge sejam instaladas na máquina do servidor.
- **HP ProLiant**
  - *Modo de visualização da política:* zz[SYS] Policy - HW_HP ProLiant
  - *Descrição:* HP ProLiant: aplica alertas e monitoramento específicos a hardware de servidor HP ProLiant. Esse monitoramento pode exigir que ferramentas específicas de monitoramento de servidor HP ProLiant sejam instaladas na máquina do servidor.
- **IBM Series x**
  - *Modo de visualização da política:* zz[SYS] Policy - HW_IBM Series X
  - *Descrição:* IBM Series x: aplica alertas e monitoramento específicos para hardware de servidor IBM Series X. Esse monitoramento pode exigir que ferramentas específicas de monitoramento de servidor IBM Series X sejam instaladas na máquina do servidor.

[System].Core.Org Specific Policies.Monitoring.Server.Roles

- **Backup Exec Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Backup Exec Server
  - *Descrição:* Backup Exec Server: aplica monitoramento a servidores de execução de backup.
- **Blackberry Enterprise Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Blackberry Server
  - *Descrição:* Blackberry Enterprise Server: aplica monitoramento a servidores Blackberry Enterprise.

- **BrightStor ARCServe Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Brightstor ARCserve Server
  - *Descrição:* BrightStor ARCServe Server: aplica monitoramento a servidores BrightStor.
- **Citrix Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Citrix Server
  - *Descrição:* Citrix Server: aplica monitoramento a servidores Citrix.
- **Servidor DHCP**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_DHCP Server
  - *Descrição:* DHCP Server: aplica monitoramento a servidores DHCP.
- **Servidor DNS**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_DNS Server
  - *Descrição:* DNS Server: aplica monitoramento a servidores DNS.
- **Controlador de domínio**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Domain Controller
  - *Descrição:* Domain Controller: aplica monitoramento a controladores de domínio.
- **Exchange 2003 Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Exchange 2003 Server
  - *Descrição:* Exchange 2003 Server: aplica monitoramento a servidores Exchange 2003.
- **Exchange 2007 Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Exchange 2007 Server
  - *Descrição:* Exchange 2007 Server: aplica monitoramento a servidores Exchange 2007.
- **Exchange 2010 Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Exchange 2010 Server
  - *Descrição:* Exchange 2010 Server: aplica monitoramento a servidores Exchange 2003.
- **Exchange Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Exchange Server
  - *Descrição:* Exchange Server: aplica monitoramento a servidores Exchange.
- **Servidor de arquivo**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_File Server
  - *Descrição:* File Server: aplica monitoramento a servidores de arquivos.
- **FTP Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_FTP Server
  - *Descrição:* FTP Server: aplica monitoramento a servidores de FTP.
- **IIS Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_IIS Server
  - *Descrição:* IIS Server: aplica monitoramento a servidores ISS.
- **IMAP4 Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_IMAP4 Server
  - *Descrição:* IMAP4 Server: aplica monitoramento a servidores IMAP4.
- **POP3 Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_POP3 Server

- *Descrição:* POP3 Server: aplica monitoramento a servidores POP3.

- **Print Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Print Server
  - *Descrição:* Print Server: aplica monitoramento a servidores de impressão.
- **SharePoint Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_SharePoint Server
  - *Descrição:* SharePoint Server: aplica monitoramento a servidores SharePoint.
- **SMTP Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_SMTP Server
  - *Descrição:* SMTP Server: aplica monitoramento a servidores SMTP.
- **Servidor SQL**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_SQL Server
  - *Descrição:* SQL Server: aplica monitoramento a servidores SQL.
- **SQL Server 2005**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_SQL Server 2005
  - *Descrição:* SQL Server 2005: aplica monitoramento a servidores SQL 2005.
- **SQL Server 2008**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_SQL Server 2008
  - *Descrição:* SQL Server 2008: aplica monitoramento a servidores SQL 2008.
- **Servidor de terminal**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_Terminal Server
  - *Descrição:* Terminal Server: aplica monitoramento a servidores de Terminal.
- **WINS Server**
  - *Modo de visualização da política:* zz[SYS] Policy - Role_WINS Server
  - *Descrição:* WINS Server: aplica monitoramento a servidores WINS.

[System].Core.Org Specific Policies.Monitoring.Workstation

- **Common Windows Workstation Monitoring**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows Workstations
  - *Descrição:* Monitoramento comum de estação de trabalho com Windows: aplica um conjunto comum de monitoramento para todas as estações de trabalho com Windows. Isso inclui log de eventos relacionados a hardware, Windows Service e monitoramento comum de desempenho do Windows.
- **Windows Workstation (Core)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows Workstations
  - *Descrição:* Estação de trabalho com Windows (Core): aplica uma variedade de monitoramentos de estações de trabalho com Windows (Core) a estações de trabalho com Windows, incluindo monitoramento de serviços padrão, desempenho do sistema, geração de relatórios de integridade e muito mais.
- **Windows Vista**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_Win Vista
  - *Descrição:* Windows Vista: aplica monitoramento de serviço padrão para máquinas com Windows Vista.
- **Windows 7**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_Win 7
  - *Descrição:* Windows 7: aplica monitoramento de serviço padrão para máquinas com Windows Vista.

- **Windows XP**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_Win XP
  - *Descrição:* Windows XP: aplica monitoramento de serviço padrão para máquinas com Windows Vista.
- **Windows 8**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_Win 8
  - *Descrição:* Windows 8: aplica monitoramento de serviço padrão para máquinas com Windows 7.

[System].Core.Org Specific Policies.Monitoring.Security.Anti-Virus

- **AVG Tech**
  - *Modo de visualização da política:* zz[SYS] Policy - AV_AVG Technologies
  - *Descrição:* McAfee: aplica monitoramento do AVG Technologies AntiVirus.
- **Kaspersky ES**
  - *Modo de visualização da política:* zz[SYS] Policy - AV_Kaspersky ES
  - *Descrição:* Kaspersky ES: aplica monitoramento do Kaspersky Endpoint Security.
- **McAfee**
  - *Modo de visualização da política:* zz[SYS] Policy - AV_McAfee
  - *Descrição:* McAfee: aplica monitoramento do McAfee AntiVirus.
- **Microsoft SE-FEP**
  - *Modo de visualização da política:* zz[SYS] Policy - AV_Microsoft SE-FEP
  - *Descrição:* Microsoft SE-FEP: aplica monitoramento do Microsoft Security Essentials e Forefront Endpoint Protection.
- **Sophos**
  - *Modo de visualização da política:* zz[SYS] Policy - AV_Sophos
  - *Descrição:* Sophos: aplica monitoramento do Sophos AntiVirus.
- **Symantec AV**
  - *Modo de visualização da política:* zz[SYS] Policy - AV_Symantec AV
  - *Descrição:* Symantec zz[SYS] AV: aplica monitoramento do Symantec AntiVirus.
- **Symantec EP**
  - *Modo de visualização da política:* zz[SYS] Policy - AV_Symantec EP
  - *Descrição:* Symantec EP: aplica monitoramento do Symantec Endpoint Protection.
- **Trend Micro**
  - *Modo de visualização da política:* zz[SYS] Policy - AV_Trend Micro
  - *Descrição:* Trend Micro: aplica monitoramento do Trend Micro AntiVirus.

[System].Core.Org Specific Policies.Monitoring.Utility

- **Atualizar listas por varredura**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows
  - *Descrição:* Atualizar listas por varredura: aplica uma atualização de listas por varredura agendada em todas as máquinas com Windows para manter informações de serviços de execução, log de eventos e contador de desempenho atualizadas para cada máquina para fins de monitoramento preciso.
- **Limpeza de monitoramento**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows
  - *Descrição:* Limpeza de monitoramento: como a última política que contém conjuntos de monitores e alertas, essa política garante efetivamente que o monitoramento aplicado

anteriormente (conjuntos de monitores e alertas de logs de eventos atribuídos através de outras políticas não mais necessários devido a alterações de função etc.) seja removido.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Common Windows Patch Mgmt Settings

- **Configurações de negação de correção**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Deny Patching Group
  - *Descrição:* Configurações de negação de correção: aplica configurações de gerenciamento de correções em máquinas selecionadas na visualização 'zz[SYS] Policy - Deny Patching Group'. Define a Ação de reinicialização como "Se o usuário estiver conectado, solicitar a reinicialização a cada 60 minutos até que esta ocorra. Reinicializar se o usuário não estiver conectado". Define a participação na Política de correções como a política de correções "Recusar correções". Define Alertas de correção para gerar um Alarme e enviar um e-mail para o endereço de e-mail de "Alertas de correção" quando houver "Falha na instalação da correção" ou "A credencial do agente é inválida ou está ausente".
- **Configurações de teste de correção**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Test Patching Group
  - *Descrição:* Configurações de teste de correção: aplica configurações de gerenciamento de correções em máquinas selecionadas na visualização 'zz[SYS] Policy - Test Patching Group'. Define a Ação de reinicialização como "Se o usuário estiver conectado, solicitar a reinicialização a cada 60 minutos até que esta ocorra. Reinicializar se o usuário não estiver conectado". Define a participação na Política de correções como a política de correções "Testar correções". Define Alertas de correção para gerar um Alarme e enviar um e-mail para o endereço de e-mail de "Alertas de correção" quando houver "Falha na instalação da correção" ou "A credencial do agente é inválida ou está ausente".
- **Desativar atualização automática do Windows**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Windows Auto Update Enabled
  - *Descrição:* desativa atualizações automáticas do Windows em máquinas que têm a Atualização automática do Windows ativada. Se a Atualização automática do Windows estiver ativada e o Kaseya Patch Management estiver sendo usado, então poderá haver um conflito da Atualização automática do Windows com a estratégia de gerenciamento de correções Kaseya, podendo resultar na implementação de correções que foram negadas ou que ainda estejam com aprovação pendente no Kaseya.
- **Origem do arquivo - Internet**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows
  - *Descrição:* Origem do arquivo - Internet: define a origem de arquivo do Patch Management como Internet para todas as máquinas com Windows, a fim de que as correções sejam obtidas por download diretamente dos servidores de correções e download da Microsoft. Essa política é o padrão e pode ser substituída por uma política alternativa que é aplicada a organizações ou grupos de máquinas específicas; também tem precedência sobre essa política.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Workstation Patch Mgmt Settings

- **Configurações de correções de estação de trabalho**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows Workstations
  - *Descrição:* Configurações de correções de estação de trabalho: aplica configurações do Patch Management a estações de trabalho com Windows. Define a Ação de reinicialização como "Se o usuário estiver conectado, solicitar a reinicialização a cada 60 minutos até que esta ocorra. Reinicializar se o usuário não estiver conectado". Define a

participação na Política de correções como a política de correções "Correções da estação de trabalho". Define Alertas de correção para gerar um Alarme e enviar um e-mail para o endereço de e-mail de "Alertas de correção" quando houver "Falha na instalação da correção" ou "A credencial do agente é inválida ou está ausente".

- **Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6am-6pm/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
  - *Descrição:* Agendamento diário de estação de trabalho para mais de 10 correções (atualização automática, de segunda a sexta, das 6h às 18h/gestão de energia): aplica agendamentos diários de atualização automática a membros da Política de correções de estação de trabalho que estão com 10 ou mais correções aprovadas ausentes. As atualizações automáticas estão agendadas para ocorrer de segunda a sexta, semanalmente, das 6h às 18h. Essa política geralmente é usada quando clientes têm máquinas que estão com algumas correções ausentes e eles querem que esses sistemas sejam atualizados ao longo de dias, em vez de semanas ou meses. Assim que as máquinas forem corrigidas não precisarão mais ter correções aplicadas diariamente. As atualizações automáticas são realizadas durante o dia para atender a clientes nos quais as máquinas geralmente são desligadas à noite, mas a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas durante o dia possam ser ativadas antes da realização dessas operações.
- **Weekly Wkst Schedule (Scan Tu 6am-6pm/Auto Update W 6am-6pm/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Descrição:* Agendamento semanal de estação de trabalho (varredura, às terças-feiras, das 6h às 18h/Atualização automática, às quartas-feiras, das 6h às 18h/gestão de energia): aplica agendamentos semanais de atualização automática e varredura de correções a membros da Política de correções de estação de trabalho. As varreduras de correção estão agendadas para que ocorram às terças-feiras, semanalmente, das 6h às 18h, e as atualizações automáticas estão agendadas para às quartas-feiras, semanalmente, das 6h às 18h. Essa política geralmente é usada quando clientes querem usar uma abordagem mais agressiva para correções, a fim de ajudar a minimizar riscos devido ao fato de máquinas não serem corrigidas e, portanto, querem que novas correções sejam implementadas relativamente rápido em máquinas. As atualizações automáticas são realizadas durante o dia para atender a clientes nos quais as máquinas geralmente são desligadas à noite, mas a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas durante o dia possam ser ativadas antes da realização dessas operações.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Server Patch Mgmt Settings

- **Configurações de correções de servidor**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows Servers
  - *Descrição:* Configurações de correções de servidor: aplica configurações de gerenciamento de correções a servidores com Windows. Define a Ação de reinicialização como "Não reinicializar após a atualização", "Quando for necessário reinicializar, enviar um e-mail para 'Alertas de correção'". Define a participação na Política de correções como a política de correções "Correções do servidor". Define Alertas de correção para gerar um Alarme e enviar um e-mail para o endereço de e-mail de "Alertas de correção" quando houver "Falha na instalação da correção" ou "A credencial do agente é inválida ou está ausente".
- **Weekly Srvr Schedule (Scan W 6pm-6am)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Windows Servers
  - *Descrição:* Agendamento semanal de servidor (varredura, semanal, das 18h às 6h): aplica agendamento de varredura de correção a membros da política de correção de

servidor. Varreduras de correção são agendadas para ocorrer às quartas-feiras, semanalmente, das 18h às 6h. Nenhuma implementação de atualização automática está agendada em servidores por esta política.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Other Windows Patch Mgmt Settings

- **Servidor do sistema - origem do arquivo**
  - *Modo de visualização da política:* zz[SYS] Policy - Network_10.11.12.x
  - *Descrição:* Origem do arquivo - Servidor do sistema: define a origem do arquivo para o gerenciamento de correções como o servidor do sistema para todas as máquinas com Windows, a fim de que as correções sejam obtidas centralmente por download pelo servidor do sistema e então distribuídas do servidor do sistema para as máquinas sendo corrigidas.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Other Windows Patch Mgmt Settings.Other Schedules.Daytime

- **Monthly Wkst Schedule (Scan 2nd W 6am-6pm/Auto Update 1st W 6am-6pm/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Descrição:* Agendamento mensal de estação de trabalho (varredura, segunda quarta-feira do mês, das 6h às 18h/atualização automática, primeira quarta-feira do mês, das 6h às 18h/gestão de energia): aplica agendamentos de atualização automática e varredura de correções a membros da Política de correções de estação de trabalho. As varreduras de correções estão agendadas para ocorrer na segunda quarta-feira do mês, das 6h às 18h. As atualizações automáticas estão agendadas para ocorrer na primeira quarta-feira do mês, das 6h às 18h. Essa política geralmente é usada quando clientes querem usar uma abordagem mais conservadora para o gerenciamento de correções, pois varreduras e atualizações são realizadas somente uma vez por mês, e atualizações são implementadas no início do mês. Isso significa que as correções sendo implementadas foram lançadas por pelo menos um mês, o que permite testes extensivos de correções antes de sua implementação geral. As varreduras e atualizações automáticas são realizadas durante o dia para atender a clientes para os quais as máquinas geralmente são desligadas à noite, mas a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas durante o dia possam ser ativadas antes da realização dessas operações.

[System].Core.Org Specific Policies.Patch / Update Management.Windows.Windows Workstation Patch Mgmt Settings.Nighttime

- **Daily Wkst Schedule for 10+ Patches (Auto Update M-F 6pm-6am/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
  - *Descrição:* Agendamento diário de estação de trabalho para mais de 10 correções (atualização automática, de segunda a sexta, das 18h às 6h/gestão de energia): aplica agendamentos diários de atualização automática a membros da Política de correções de estação de trabalho que estão com 10 ou mais correções aprovadas ausentes. As atualizações automáticas estão agendadas para ocorrer de segunda a sexta, semanalmente, das 18h às 6h. Essa política geralmente é usada quando clientes têm máquinas que estão com algumas correções ausentes e eles querem que esses sistemas sejam atualizados ao longo de dias, em vez de semanas ou meses. Assim que as máquinas forem corrigidas não precisarão mais ter correções aplicadas diariamente. As atualizações automáticas são realizadas durante a noite para ajudar a minimizar a interrupção de serviço, e a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas possam ser ativadas antes da realização dessas operações.

- **Weekly Wkst Schedule for 10+ Patches (Auto Update W 6pm-6am/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Workstation Patching Policy Missing 10+ Patches
  - *Descrição:* Agendamento semanal de estação de trabalho para mais de 10 correções (atualização automática, às quartas-feiras, das 18h às 6h/gestão de energia): aplica agendamentos semanais de atualização automática a membros da Política de correções de estação de trabalho que estão com 10 ou mais correções aprovadas ausentes. Atualizações automáticas são agendadas para ocorrer às quartas-feiras, semanalmente, das 18h às 6h. Essa política geralmente é usada quando clientes têm máquinas que estão com algumas correções ausentes e eles querem que esse sistemas sejam atualizados ao longo de semanas, em vez de meses. Assim que as máquinas forem corrigidas, elas não precisarão mais serem corrigidas semanalmente e se encaixarão novamente em um agendamento mensal de atualização automática e varredura de correções. As atualizações automáticas são realizadas durante a noite para atender a clientes nos quais as máquinas geralmente são desligadas à noite, mas a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas durante o dia possam ser ativadas antes da realização dessas operações.
- **Weekly Wkst Schedule (Scan Tu 6pm-6am/Auto Update W 6pm-6am/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Descrição:* Agendamento semanal de estação de trabalho (varredura, às terças-feiras, das 18h às 6h/Atualização automática, às quartas-feiras, das 18h às 6h/gestão de energia): aplica agendamentos semanais de atualização automática e varredura de correções a membros da Política de correções de estação de trabalho. As varreduras de correção estão agendadas para que ocorram às terças-feiras, semanalmente, das 18h às 6h, e as atualizações automáticas estão agendadas para às quartas-feiras, semanalmente, das 18h às 6h. Essa política geralmente é usada quando clientes querem usar uma abordagem mais agressiva para correções, a fim de ajudar a minimizar riscos devido ao fato de máquinas não serem corrigidas e, portanto, querem que novas correções sejam implementadas relativamente rápido em máquinas. As varreduras e atualizações automáticas são realizadas durante a noite para ajudar a minimizar a interrupção de serviço, e a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas possam ser ativadas antes da realização dessas operações.
- **Monthly Wkst Schedule (Scan 2nd W 6pm-6am/Auto Update 1st W 6pm-6am/Power Mgmt)**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Workstation Patching Policy
  - *Descrição:* Agendamento mensal de estação de trabalho (varredura, segunda quarta-feira do mês, das 18h às 6h/atualização automática, primeira quarta-feira do mês, das 18h às 6h/gestão de energia): aplica agendamentos de atualização automática e varredura de correções a membros da Política de correções de estação de trabalho. As varreduras de correções estão agendadas para ocorrer na segunda quarta-feira do mês, das 18h às 6h. As atualizações automáticas estão agendadas para ocorrer na primeira quarta-feira do mês, das 18h às 6h. As varreduras e atualizações automáticas são realizadas durante a noite para ajudar a minimizar a interrupção de serviço, e a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas possam ser ativadas antes da realização dessas operações. Essa política geralmente é usada quando clientes querem usar uma abordagem mais conservadora para o gerenciamento de correções, pois varreduras e atualizações são realizadas somente uma vez por mês, e atualizações são implementadas no início do mês. Isso significa que as correções sendo implementadas foram lançadas por pelo menos um mês, o que permite testes extensivos de correções antes de sua implementação geral.
- **Monthly Srvr Schedule (Scan 2nd W 6pm-6am)**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Server Patching Policy

- *Descrição:* Agendamento mensal de servidor (varredura, segunda quarta-feira do mês, das 18h às 6h): aplica agendamento de varredura de correção a membros da política de correção de servidor. As varreduras de correções estão agendadas para ocorrer na segunda quarta-feira do mês, das 18h às 6h. Nenhuma implementação de atualização automática está agendada em servidores por esta política.

- **Monthly Srvr Schedule (Scan 2nd W 6pm-6am/Auto Update 1st Su 12am-4am)**
  - *Modo de visualização da política:* zz[SYS] Policy - Patch_Server Patching Policy
  - *Descrição:* Agendamento mensal de servidor (varredura, segunda quarta-feira do mês, das 18h às 6h/atualização automática, primeiro domingo do mês, da meia-noite às 4h): aplica agendamentos de atualização automática e varredura de correções a membros da Política de correções de servidor. As varreduras de correções estão agendadas para ocorrer na segunda quarta-feira do mês, das 6h às 18h. As atualizações automáticas estão agendadas para ocorrer no primeiro domingo do mês, da meia-noite às 4h. Essa política geralmente é usada quando clientes querem usar uma abordagem mais conservadora para o gerenciamento de correções, pois varreduras e atualizações são realizadas somente uma vez por mês, e atualizações são implementadas no início do mês. Isso significa que as correções sendo implementadas foram lançadas por pelo menos um mês, o que permite testes extensivos de correções antes de sua implementação geral. As varreduras e atualizações automáticas são realizadas no fim de semana, no início da amanhã, para que o tempo de produção e os usuários sejam menos afetados por quaisquer interrupções de serviço relacionadas a servidores de correções.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Workstation Software Update Settings

- **Weekly Macintosh Workstation Software Update (Install Recommended W 6am-6pm)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Descrição:* Atualização semanal de software de estação de trabalho Macintosh (instalação recomendada, às quartas-feiras, das 6h às 18h): aplica uma atualização de software Mac para execução às quartas-feiras, das 6h às 18h, todas as semanas, que instalará atualizações de software Macintosh recomendadas em estações de trabalho Macintosh. As atualizações de software são realizadas durante o dia para atender a clientes nos quais as máquinas geralmente são desligadas à noite, mas a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas durante o dia possam ser ativadas antes da realização dessas operações.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Macintosh Server Software Update Settings

- **Monthly Macintosh Server Software Update (Install Recommended 1st Su 12am-4am)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Mac OS X Servers
  - *Descrição:* Atualização mensal de software de servidor Macintosh (instalação recomendada, primeiro domingo do mês, da meia-noite às 4h: aplica uma atualização de software Mac para execução no primeiro domingo do mês, que instalará atualizações de software Macintosh recomendadas em servidores Macintosh. Isso irá manter os servidores Mac atualizados com atualizações recomendadas.

[System].Core.Org Specific Policies.Patch / Update Management.Macintosh.Other Macintosh Software Update Settings

- **Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6am-6pm)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Descrição:* Atualização mensal de software de estação de trabalho Macintosh (instalação recomendada, na primeira quarta-feira do mês, das 6h às 18h): aplica uma atualização de software Mac para execução na primeira quarta-feira de cada mês, das 6h às 18h, que instalará atualizações de software Macintosh recomendadas em estações de

trabalho Macintosh. As atualizações de software são realizadas durante o dia para atender a clientes nos quais as máquinas geralmente são desligadas à noite, mas a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas durante o dia possam ser ativadas antes da realização dessas operações.

- **Monthly Macintosh Workstation Software Update (Install Recommended 1st W 6pm-6am)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Descrição:* Atualização mensal de software de estação de trabalho Macintosh (instalação recomendada, na primeira quarta-feira do mês, das 18h às 6h): aplica uma atualização de software Mac para execução na primeira quarta-feira de cada mês, das 18h às 6h, que instalará atualizações de software Macintosh recomendadas em estações de trabalho Macintosh. As atualizações de software são realizadas durante a noite para ajudar a minimizar a interrupção de serviço, e a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas possam ser ativadas antes da realização dessas operações.
- **Monthly Macintosh Workstation Software Update (Install All 1st W 6pm-6am)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Mac OS X Workstations
  - *Descrição:* Atualização mensal de software de estação de trabalho Macintosh (instalação completa, na primeira quarta-feira do mês, das 18h às 6h): aplica uma atualização de software Mac para execução na primeira quarta-feira de cada mês, das 18h às 6h, que instalará todas as atualizações de software Macintosh em estações de trabalho Macintosh. As atualizações de software são realizadas durante a noite para ajudar a minimizar a interrupção de serviço, e a opção de gestão de energia está ativada nesses agendamentos para que quaisquer máquinas desligadas possam ser ativadas antes da realização dessas operações.

[System].Core.Org Specific Policies.Patch / Update Management.Linux

- **Monthly Linux Package Updates/Upgrades (Install 1st W 6pm-6am)**
  - *Modo de visualização da política:* zz[SYS] Policy - OS_All Linux
  - *Descrição:* Atualizações/upgrades mensais de pacote Linux (Instalação na primeira quarta-feira do mês, das 18h às 6h): aplica um procedimento de atualização/upgrade de pacotes Linux para execução na primeira quarta-feira do mês. Isso manterá as máquinas Linux atualizadas e com as versões mais recentes de vários componentes de software instalados.

Detalhes da política de correções

Recusar correções	Política de aprovação padrão
Atualização de Segurança ? Crítica (Alta Prioridade)	Negado
Atualização de Segurança ? Importante (Alta Prioridade)	Negado
Atualização de Segurança ? Moderada (Alta Prioridade)	Negado
Atualização de Segurança ? Baixa (Alta Prioridade)	Negado
Atualização de Segurança ? Não Classificada (Alta Prioridade)	Negado
Atualização Crítica (Alta Prioridade)	Negado
Implementação de Atualização (Alta Prioridade)	Negado
Service Pack (Opcional - Software)	Negado
Atualização (Opcional - Software)	Negado
Pacote de Funcionalidades (Opcional - Software)	Negado

Ferramenta (Opcional - Software)	Negado

Correções de servidor

Atualização de Segurança ? Crítica (Alta Prioridade)	Aprovação pendente
Atualização de Segurança ? Importante (Alta Prioridade)	Aprovação pendente
Atualização de Segurança ? Moderada (Alta Prioridade)	Aprovação pendente
Atualização de Segurança ? Baixa (Alta Prioridade)	Aprovação pendente
Atualização de Segurança ? Não Classificada (Alta Prioridade)	Aprovação pendente
Atualização Crítica (Alta Prioridade)	Aprovação pendente
Implementação de Atualização (Alta Prioridade)	Aprovação pendente
Service Pack (Opcional - Software)	Aprovação pendente
Atualização (Opcional - Software)	Aprovação pendente
Pacote de Funcionalidades (Opcional - Software)	Aprovação pendente
Ferramenta (Opcional - Software)	Aprovação pendente

Testar correções

Atualização de Segurança ? Crítica (Alta Prioridade)	Aprovado
Atualização de Segurança ? Importante (Alta Prioridade)	Aprovado
Atualização de Segurança ? Moderada (Alta Prioridade)	Aprovado
Atualização de Segurança ? Baixa (Alta Prioridade)	Aprovado
Atualização de Segurança ? Não Classificada (Alta Prioridade)	Aprovado
Atualização Crítica (Alta Prioridade)	Aprovado
Implementação de Atualização (Alta Prioridade)	Aprovação pendente
Service Pack (Opcional - Software)	Aprovação pendente
Atualização (Opcional - Software)	Aprovação pendente
Pacote de Funcionalidades (Opcional - Software)	Aprovação pendente
Ferramenta (Opcional - Software)	Aprovação pendente

Correções de estação de trabalho

Atualização de Segurança ? Crítica (Alta Prioridade)	Aprovado
Atualização de Segurança ? Importante (Alta Prioridade)	Aprovado
Atualização de Segurança ? Moderada (Alta Prioridade)	Aprovado
Atualização de Segurança ? Baixa (Alta Prioridade)	Aprovado
Atualização de Segurança ? Não Classificada (Alta Prioridade)	Aprovado
Atualização Crítica (Alta Prioridade)	Aprovado
Implementação de Atualização (Alta Prioridade)	Aprovação pendente
Service Pack (Opcional - Software)	Aprovação pendente
Atualização (Opcional - Software)	Aprovação pendente
Pacote de Funcionalidades (Opcional - Software)	Aprovação pendente
Ferramenta (Opcional - Software)	Aprovação pendente

Procedimentos do agente

Nesta seção

Core.0 Common Procedures

Core.0 Common Procedures.Reboot/Shutdown/Logoff

- **Forçar o logoff do usuário**
  - Efetua o logoff do usuário atualmente conectado.
- **Reinicializar-Perguntar-Não**
  - Se o usuário estiver conectado, perguntar se está OK para reinicializar; assumir Não após 5 minutos. Se o usuário estiver conectado, siga em frente e reinicialize. Este script chama Reinicializar-Perguntar-Não-2 para perguntar ao usuário.
- **Reinicializar-Perguntar-Não-2**
  - *** NÃO PROGRAMAR ESTE SCRIPT!! ***Este script é chamado pelo script Reboot-Ask-No e não pode ser programado por si próprio.
- **Reinicializar-Perguntar-Sim**
  - Se o usuário estiver conectado, perguntar se está OK para reinicializar; assumir Sim após 5 minutos. Se o usuário não estiver conectado, siga em frente e reinicialize. Este script chama Reinicializar-Perguntar-Sim-2 para perguntar ao usuário.
- **Reinicializar-Perguntar-Sim-2**
  - *** NÃO PROGRAMAR ESTE SCRIPT!! ***Este script é chamado pelo script Reboot-Ask-Yes e não pode ser programado por si próprio.
- **Forçar a reinicialização**
  - Força uma reinicialização imediata.
- **Reinicializar-Nag**
  - Se o usuário está conectado, solicitar reinicializar a cada 5 minutos até que o usuário permita a reinicialização. Se o usuário não está conectado, siga em frente e reinicialize. Este script chama Reinicializar-Nag-2 para perguntar ao usuário.
- **Reinicializar-Nag-2**
  - *** NÃO PROGRAMAR ESTE SCRIPT!! ***Este script é chamado pelo script Reboot-Nag e não pode ser programado por si próprio.
- **Reinicializar-Não-Usuário**
  - Reinicializa a máquina somente se o usuário não estiver conectado.
- **Reinicializar-Avisar**
  - Se o usuário estiver conectado, avisa-o sobre a reinicialização em 5 minutos. Caso contrário, segue em frente e prossegue com a reinicialização.
- **Reinicializar: solicitar que usuário reinicie a cada 15 minutos até que responda Sim**
  - Este script solicitará uma reinicialização a cada 15 minutos.
- **Desligamento do computador**
  - Desliga a máquina do agente usando o utilitário shutdown.exe do Windows.

Core.1 Windows Procedures

Core.1 Windows Procedures.Desktops.Auditing

- **Auditar informações da BIOS via WMI**
  - Usa WMIC para obter informações da BIOS, grava isso em um arquivo e recupera o arquivo na pasta GetFile do sistema; em seguida, grava uma entrada no log de procedimentos do agente com as informações da BIOS detectadas.
- **Auditar BOOT.INI**
  - Realiza uma auditoria do conteúdo de C:\BOOT.INI, caso exista, grava uma entrada no log de procedimentos do agente e recupera uma cópia do BOOT.INI na pasta GetFiles do sistema.
- **Auditar arquivos (quaisquer tipos de arquivo inseridos)**
  - Pesquisa todos os arquivos usando um conjunto de máscaras de arquivo que você insere ao agendar o procedimento e cria um arquivo de log TXT simples, bem como um arquivo CSV com base nos nomes de arquivos que você também insere e que relaciona os arquivos encontrados com nome de arquivo/caminho completo, data e hora do último acesso, tamanho em bytes, proprietário e nome de arquivo.
    - ✓ Os arquivos resultantes são criados na pasta #agenttemp# definida na Etapa 1.
    - ✓ O nome do arquivo de log TXT é definido pela variável #logfile# na Etapa 2.
    - ✓ O nome do arquivo CSV é definido pela variável #csvfile# na Etapa 3.
    - ✓ As máscaras de arquivo são definidas pela variável #filemasks# na Etapa 4.
    - ✓ Ambos os arquivos resultantes são enviados para o servidor Kaseya para análise sob a pasta Documentos do perfil de máquinas.
    - ✓ O arquivo de log TXT também é gravado no log de scripts para fins de geração de relatórios.
    - ✓ Esse script pode ser compatível com alertas para alterações de arquivos, bem como alterações de etapas.
- **Auditar arquivos (PST e OST)**
  - Pesquisa todos os arquivos PST/OST usando um conjunto de máscaras de arquivos e cria um arquivo de log TXT, bem como um arquivo CSV relacionando os arquivos encontrados com nome de arquivo/caminho completo, data e hora do último acesso, tamanho em bytes, proprietário e nome de arquivo.
    - ✓ Os arquivos resultantes são criados na pasta #agenttemp# definida na Etapa 1.
    - ✓ O nome do arquivo de log TXT é definido pela variável #logfile# na Etapa 2.
    - ✓ O nome do arquivo CSV é definido pela variável #csvfile# na Etapa 3.
    - ✓ As máscaras de arquivo são definidas pela variável #filemasks# na Etapa 4.
    - ✓ Ambos os arquivos resultantes são enviados para o servidor Kaseya para análise sob a pasta Documentos do perfil de máquinas.
    - ✓ O arquivo de log TXT também é gravado no log de scripts para fins de geração de relatórios.
    - ✓ Esse script pode ser compatível com alertas para alterações de arquivos, bem como alterações de etapas.
- **Auditar velocidade de Internet (WEB100CLT)**
  - Usa o utilitário cliente NDT para Windows (web100clt.exe). Conecta-se ao servidor NDT público que você insere ao executar/agendar o procedimento (consulte http://e2epi.internet2.edu/ndt/ndt-server-list.html para obter uma lista de servidores) e realiza um teste de velocidade de Internet (ascendente/descendente), bem como outros diagnósticos de rede. O arquivo resultante (Internet_Speed.txt) é recuperado na pasta GetFile do sistema.

- **Auditar chave de registro IRPStackSize**
  - Realiza uma auditoria do valor IRPStackSize. A ID de evento 2011 pode ser causada por antivírus e por vários outros tipos de software. Consulte http://support.microsoft.com/kb/177078.
- **Auditar contas admin locais**
  - Registra em log as contas de usuário que são parte do grupo Administradores na máquina local no log de procedimentos do agente.
- **Auditar contas de guests locais**
  - Registra em log as contas de usuário que são parte do grupo Guests na máquina local no log de procedimentos do agente. Se as contas forem relatadas, elas serão ativadas.
- **Auditar contas de usuários locais**
  - Registra em log as contas de usuários definidas na máquina no log de procedimentos do agente.
- **Auditar contagem de arquivos MP3**
  - Conta o número de arquivos MP3 na unidade C: da máquina e grava uma entrada no log de procedimentos do agente indicando esse número.
- **Auditar portas TCP abertas e ouvintes**
  - Audita portas TCP abertas e ouvintes no Windows usando NETSTAT e, em seguida, recupera os resultados na pasta GetFile do sistema.
- **Auditar locais PageFile**
  - Audita os locais PageFile em máquinas Windows e grava uma entrada no log de procedimentos do agente com as informações.
- **Auditar serviços em execução (NET START)**
  - Audita os serviços atualmente iniciados em uma máquina com Windows e recupera a lista desses serviços na pasta GetFile do sistema.
- **Auditar serviços (SC QUERY)**
  - Usa SC QUERY para auditar a lista de Serviços Windows em um arquivo e recupera o arquivo na pasta GetFile do sistema.
- **Auditar chave de registro de serviços**
  - Use o comando REG para consultar a chave de registro HKLM\System\CurrentControlSet\Services de um agente e recupere os resultados na pasta GetFile do sistema.
- **Auditar a chave do registro de desinstalação**
  - Usa o comando REG para consultar a chave de registro HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall da máquina e recupere os resultados na pasta GetFile do sistema.
- **Auditar dispositivos Plug-N-Play USB**
  - Usa VBS e WMI (classe Win32_PnPEntity) para auditar os serviços USB em uma máquina com Windows. Os resultados são recuperados na pasta GetFile do sistema.
- **Auditar resolução de vídeo do usuário**
  - Usa VBS para auditar a configuração de resolução do monitor de vídeo dos usuários atuais. Grava o resultado no log de procedimentos do agente, bem como em um campo de informações personalizadas do sistema chamado de resolução de vídeo do usuário.
- **Auditar informações do monitor Windows**
  - Usa VBS e WMI (classe root\CIMV2:Win32_DesktopMonitor) para auditar informações do monitor Windows. Grava a saída em um arquivo e recupera o arquivo na pasta GetFile do sistema.
- **Auditar informações de EDID do monitor Windows**

- Usa VBS com WMI para detectar informações de EDID do monitor (fabricante do monitor, modelo do monitor e número de série do monitor) e grava as informações detectadas no log de procedimentos do agente e nos campos de informações personalizadas do sistema.

Core.1 Windows Procedures.Desktops.Auditing.Share and NTFS

- **Auditar todas as sessões de compartilhamento e usuários (NET SESSION)**
  - Usa NET SESSION para despejar uma lista básica das sessões em compartilhamentos em um agente e a envia para a pasta Docs\Shares-NTFS a fim de que os arquivos possam ser visualizados via a guia de resumo da máquina/função Documentos.
- **Auditar todos os arquivos compartilhados abertos e usuários (NET FILE)**
  - Usa NET FILE para despejar uma lista básica dos arquivos abertos de todos os compartilhamentos em um agente e a envia para a pasta Docs\Shares-NTFS, a fim de que os arquivos possam ser visualizados via a guia de resumo da máquina/função Documentos.
- **Auditar todos os compartilhamentos (NET SHARE)**
  - Usa NET SHARE para despejar uma lista básica dos compartilhamentos em um agente e a envia para a pasta Docs\Shares-NTFS, a fim de que os arquivos possam ser visualizados via a guia de resumo da máquina/função Documentos.
- **Auditar permissões de pasta de usuário/grupo vigentes (ACCESSCHK)**
  - Usa ACCESSCHK de Microsoft SysInternals para verificar as permissões vigentes de um PC local/usuário de domínio/objeto de grupo em uma pasta. Edite esse script nas etapas 2 a 6 para essas variáveis:

    pcdom = nome do computador ou nome de domínio do usuário ou grupo
    usrgrp = nome de usuário ou nome de grupo para avaliar
    drive = letra da unidade na qual a pasta está
    folder = caminho completo da pasta a ser auditada
    fldrdesc = um nome descritivo da pasta a ser auditada (sem caracteres especiais).
- **Auditar compartilhamentos não administrativos (SRVCHECK)**
  - Usa SRVCHECK para despejar uma lista básica dos compartilhamentos não administrativos em um agente e a envia para a pasta Docs\Shares-NTFS, a fim de que os arquivos possam ser visualizados via a guia de resumo da máquina/função Documentos.
- **Auditar pastas compartilhadas (DUMPSEC)**
  - Usa DUMPSEC para criar um relatório de todos os compartilhamentos com seus caminhos, contas, proprietários e permissões de acesso, e o envia para a pasta Docs\Shares-NTFS, a fim de que os arquivos possam ser visualizados via a guia de resumo da máquina/função Documentos.
- **Auditar ACLs e pastas compartilhadas (VBS/WMI)**
  - Usa VBS com WMI para auditar todos os compartilhamentos locais, compartilhamentos e permissões de NTFS.
- **Auditar impressoras compartilhadas (DUMPSEC)**
  - Usa DUMPSEC para criar um relatório de todas as impressoras com nomes, contas, proprietários e permissões de acesso, e o envia para a pasta Docs\Shares-NTFS, a fim de que os arquivos possam ser visualizados via a guia de resumo da máquina/função Documentos.

Core.1 Windows Procedures.Desktops.Auditing.Share and NTFS.Audit Admin Shares

- **Auditar compartilhamentos administrativos automáticos**
  - Usa NET SHARE para auditar compartilhamentos administrativos automáticos, como C$ etc. Os resultados são recuperados na pasta Documentos do sistema sob uma subpasta Compartilhamento-NFTS.
- **Auditar configuração de compartilhamentos administrativos automáticos**

- Com base no SO da máquina, verifica a existência e o valor de AutoShareServer ou AutoShareWkst no registro do Windows e grava uma entrada no log de procedimentos do agente, indicando se esse recurso está ativado ou desativado.

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.Dell

- **Inventário de configurações de BIOS Dell via DCCU**
  - Usa o Dell Client Configuration Utility (DCCU) para realizar o inventário da BIOS de uma máquina de nível empresarial Dell. Os resultados são recuperados na pasta GetFile do sistema.
- **Definir configurações de BIOS Dell via DCCU**
  - Define configurações da BIOS Dell com base na configuração e no valor fornecidos quando agendados. O formato da configuração da BIOS Dell fornecido deve ser o usado pelo Dell Client Configuration Utility (DCCU).

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.HP

- **HP BiosConfigUtility GetConfig**
  - Usa o HP Bios Config Utility para realizar o inventário da BIOS de uma máquina de nível empresarial HP. Os resultados são recuperados na pasta GetFile do sistema.

Core.1 Windows Procedures.Desktops.Machine Control.BIOS Management.Lenovo

- **Obter configurações da BIOS Lenovo via WMI-VBS**
  - Usa VBS e WMI para obter todas as configurações da BIOS em sistemas Lenovo.
- **Definir configurações da BIOS Lenovo via WMI-VBS**
  - Usa VBS e WMI para obter configurações da BIOS em sistemas Lenovo. Solicita o nome e o valor de configuração da BIOS Lenovo quando executada/agendada.

Core.1 Windows Procedures.Desktops.Machine Control.File Sharing

- **Desativar compartilhamento de arquivos simples (define ForceGuest=0) em Windows XP**
  - Desativa o recurso de compartilhamento de arquivos simples (define ForceGuest=0) em sistemas Windows XP e, depois disso, interrompe e reinicia o serviço de servidor para que a alteração seja implementada.
- **Ativar compartilhamentos administrativos automáticos**
  - Ativa o recurso AutoShareWks em estações de trabalho Windows para que compartilhamentos administrativos sejam criados automaticamente quando o serviço de servidor iniciar. Este procedimento do agente NÃO reinicia o serviço de servidor (lanmanserver).
- **Ativar compartilhamento de arquivos simples (define ForceGuest=1) em Windows XP**
  - Ativa o recurso de compartilhamento de arquivos simples (ForceGuest=1) em sistemas Windows XP e, depois disso, interrompe e reinicia o serviço de servidor para que a alteração seja implementada.
- **Desativar compartilhamentos administrativos automáticos**
  - Desativa o recurso AutoShareWks em estações de trabalho Windows para que compartilhamentos administrativos sejam criados automaticamente quando o serviço de servidor iniciar. Este procedimento do agente NÃO reinicia o serviço de servidor (lanmanserver).

Core.1 Windows Procedures.Desktops.Machine Control.File System

- **Converter sistema de arquivos na unidade em NTFS**
  - Converte o formato do sistema de arquivos na unidade do sistema (ou seja, a partição de inicialização) de FAT/FAT32 a NTFS. Isso funciona somente nos sistemas operacionais compatíveis com NTFS (Windows NT4/2000/XP/2003/Vista).

- **Excluir arquivos com base na data de modificação**
  - Solicita a idade de arquivos para exclusão, unidade\caminho completo para início da operação de exclusão e uma máscara de arquivo para exclusão. Em seguida, usa FORFILES para processar recursivamente todas as pastas na unidade/caminho completo inserido, excluindo arquivos que correspondem à máscara de arquivos se forem mais antigos do que a idade inserida.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Block Websites

- **Bloquear "qualquer" site**
  - Este script editará o arquivo de hosts do Windows e indicará qualquer site que você inserir no aviso para o host local, bloqueando fundamentalmente o acesso ao site desse endpoint. Isso pode ser útil para funcionários que tentam melhorar a produtividade.
- **Apagar todos os sites bloqueados**
  - Usado para remover todas as edições do arquivo de hosts do Windows. Atualiza as configurações de arquivo de hosts padrão.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Diagnostics

- **Teste de diagnóstico de rede (NETSH)**
  - Usa NETSH para realizar um teste de diagnóstico de rede e recupera os resultados na pasta Documentos do sistema, sob uma subpasta Diagnósticos de rede.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Network Connection

- **Configurar conexão de área local para utilizar DHCP**
  - Usa NETSH para alterar a configuração da conexão de rede do Windows chamada de "conexão de área local" para utilizar DHCP para suas configurações de endereço IP, DNS e WINS.
- **Corrigir prioridade DNS de RAS**
  - Corrige o problema de prioridade de vínculo de DNS de RAS, descrito em http://support.microsoft.com/kb/311218/en-us.
- **Obter configuração IP do Windows (IPCONFIG /ALL)**
  - Usa IPCONFIG /ALL para obter a configuração de endereços IP de todas as conexões de rede ativadas em uma máquina com Windows. Os resultados são recuperados na pasta GetFile do sistema.
- **Liberar e renovar endereço IP**
  - Usa um arquivo em lote para liberar e renovar um endereço IP de máquinas com Windows.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Dell

- **Ativar Wake-On-LAN na BIOS da Dell (DCCU)**
  - Usa o Dell Client Configuration Utility (DCCU) para ativar Wake-On-LAN da BIOS de máquinas de nível empresarial Dell.
- **Ativar Wake-On-LAN na BIOS da Dell (CCTK)**
  - Usa o Dell Client Configuration Tool Kit (CCTK) para ativar Wake-On-LAN da BIOS de máquinas de nível empresarial Dell.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.HP

- **Ativar Wake-On-LAN na BIOS da HP**
  - Usa o HP BIOS Configuration Utility para ativar Wake-On-LAN da BIOS de máquinas de nível empresarial HP.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Lenovo

- **Ativar Wake-On-LAN na BIOS da Lenovo**

- Usa VBS e WMI para ativar Wake-On-LAN na BIOS de máquinas de nível empresarial da Lenovo.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wake-On-LAN.Windows

- **Ativar Wake-On-LAN em Windows para todas as NICs**
  - Usa VBS para ativar o recurso Wake-On-LAN de gestão de energia em cada interface de rede do Windows. Isso permite que a máquina seja ativada através de um pacote especial quando hibernadas ou suspensas. Os recursos de WOL na BIOS também devem ser ativados para que WOL funcione.

Core.1 Windows Procedures.Desktops.Machine Control.Networking.Wireless

- **Desativar dispositivos de rede sem fio**
  - Usa DEVCON.EXE para desativar dispositivos de rede sem fio em um sistema Windows.
- **Ativar dispositivos de rede sem fio**
  - Usa DEVCON.EXE para ativar dispositivos de rede sem fio em um sistema Windows.
- **Desativar NIC em conexão de rede sem fio**
  - Usa NETSH para desativar a NIC associada à conexão de rede do Windows chamada de "conexão de rede sem fio".
- **Ativar NIC em conexão de rede sem fio**
  - Usa NETSH para ativar a NIC associada à conexão de rede do Windows chamada de "conexão de rede sem fio".

Core.1 Windows Procedures.Desktops.Machine Control.Reboot/Shutdown

- **Hibernar agora**
  - Faz com que uma máquina com Windows entre imediatamente no estado de hibernação.
- **Suspender agora**
  - Faz com que uma máquina com Windows entre imediatamente no estado de suspensão.
- **Anular desligamento**
  - Encerra o computador usando Shutdown.exe
- **Desligamento em 60 segundos**
  - Desliga o computador usando Shutdown.exe em 60 segundos.
- **Bloquear área de trabalho**
  - Faz com que a área de trabalho de máquinas com Windows seja bloqueada, exigindo credenciais de usuário atualmente conectado para desbloqueá-la.

Core.1 Windows Procedures.Desktops.Machine Control.System Restore

- **Relacionar todos os pontos de restauração do sistema**
  - Usa WMIC para enumerar todos os pontos de restauração do sistema e recupera a lista na pasta GetFile do sistema.
- **Ativar restauração do sistema em todas as unidades**
  - Usa DISKPART para enumerar todas as partições locais e, em seguida, alimenta essa lista de unidades em WMIC para desativar a restauração do sistema em cada volume. Isso removerá quaisquer pontos de restauração do sistema existentes.
- **Desativar todas as unidades de restauração do sistema**
  - Usa DISKPART para enumerar todas as partições locais e, em seguida, alimenta essa lista de unidades em WMIC para desativar a restauração do sistema em cada volume. Isso removerá quaisquer pontos de restauração do sistema existentes.
- **Criar um ponto de restauração do sistema indicado**
  - Usa WMIC para criar um ponto de restauração do sistema.

Core.1 Windows Procedures.Desktops.Machine Control.Trusted Sites

- **Adicionar sites confiáveis**
  - Executa um procedimento de registro nas máquinas para permitir que qualquer componente do domínio execute o ActiveX. Neste exemplo, ele adiciona Kaseya.net.

Core.1 Windows Procedures.Desktops.Machine Control.USB/Disk Drive Control

- **Desativar unidades USB**
  - **Deve reinicializar o endpoint depois de fazer a alteração via script** Há uma alteração de registro simples que impede que drivers de armazenamento USB iniciem quando o sistema inicia. Impede que pessoas se dirijam a um PC e copiem dados com uma chave USB, mas permite que você mantenha seu scanner, teclado e mouse funcionando.
  - Como sempre, faça backup do sistema antes de modificar o registro. Basta abrir o regedit e procurar essa chave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor Observe que o valor 'Start' alterna esse valor para 4, e dispositivos de armazenamento USB são desativados. Alterne esse valor para 3 e os dispositivos de armazenamento USB serão ativados.
- **Ativar unidades USB**
  - **Deve reinicializar o endpoint depois de fazer a alteração via script** Há uma alteração de registro simples que impede que drivers de armazenamento USB iniciem quando o sistema inicia. Impede que pessoas se dirijam a um PC e copiem dados com uma chave USB, mas permite que você mantenha seu scanner, teclado e mouse funcionando.
  - Como sempre, faça backup do sistema antes de modificar o registro. Basta abrir o regedit e procurar essa chave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor Observe que o valor 'Start' alterna esse valor para 4, e dispositivos de armazenamento USB são desativados. Alterne esse valor para 3 e os dispositivos de armazenamento USB serão ativados.
- **Desativar proteção de gravação em unidades USB**
  - Desativa proteção de gravação em dispositivos USB em máquinas com Windows executando XP SP2 ou SOs de versão posterior (consulte http://technet.microsoft.com/en-us/library/bb457157.aspx)
- **Ativar proteção de gravação em unidades USB**
  - Ativa proteção de gravação em dispositivos USB em máquinas com Windows executando XP SP2 ou SOs de versão posterior (consulte http://technet.microsoft.com/en-us/library/bb457157.aspx)
- **Desativar unidades de CD-ROM**
  - Desativa dispositivos de disco de CD-ROM.
- **Ativar unidades de CD-ROM**
  - Ativa dispositivos de disco de CD-ROM.
- **Desativar unidades flexíveis de alta capacidade**
  - Desativa dispositivos de unidade flexível de alta capacidade.
- **Ativar unidades flexíveis de alta capacidade**
  - Ativa dispositivos de unidade flexível de alta capacidade.
- **Desativar unidades de discos flexíveis**
  - Desativa dispositivos de discos flexíveis.
- **Ativar unidades de discos flexíveis**
  - Ativa dispositivos de discos flexíveis.
- **Restringir acesso à área de trabalho**

- Restringe o acesso à "Área de trabalho" no Explorer. A "Área de trabalho" aparecerá vazia e os usuários não poderão acessá-la.
- **Cancelar restrição de acesso à área de trabalho**
  - Restringe o acesso à "Área de trabalho" no Explorer. A "Área de trabalho" aparecerá vazia e os usuários não poderão acessá-la.
- **Ocultar e restringir acesso a todas as unidades (A-Z) no Explorer**
  - Usa configurações de registro NoViewOnDrive e NoDrives para ocultar e restringir acesso a todas as letras de unidade, de A a Z, em uma máquina com Windows.
- **Ocultar e restringir acesso às unidades C e D no Explorer**
  - Você pode escolher "Bloquear somente C" ou "Bloquear somente D" ou "Bloquear todas as unidades" com um dos vários procedimentos "01.Block"
- **Ocultar e restringir acesso a qualquer lista de unidades no Explorer**
  - Você pode escolher "Bloquear somente C" ou "Bloquear somente D" ou "Bloquear todas as unidades" com um dos vários procedimentos "01.Block"
- **Cancelar ocultar e restringir acesso a todas as unidades (A-Z) no Explorer**
  - Remove restrições anteriores de acesso a unidades que podem estar vigentes.
  - Nota: o Windows é compatível com a capacidade de bloquear acesso à visualização de várias letras de unidade no Explorer. Essa restrição impede usuários de utilizar Meu computador ou o Explorer para acessar o conteúdo de unidades selecionadas. Além disso, eles não podem usar o comando Executar, Mapear unidade de rede ou Dir para visualizar os diretórios nessas unidades. Este procedimento do agente remove qualquer restrição relacionada a isso.

Core.1 Windows Procedures.Desktops.Machine Control.User Access Control

- **Definir UAC (User Access Control, Controle de acesso de usuário) para sempre notificar**
  - Define o controle de acesso de usuário como Sempre notificar no Windows Vista, Windows 7 e Windows 8.
- **Definir UAC para notificar por padrão**
  - Define o controle de acesso de usuário como notificar por padrão no Windows Vista, Windows 7 e Windows 8.
- **Definir UAC para notificar no caso de não segurança**
  - Define o controle de acesso de usuário como notificar no caso de não segurança no Windows Vista, Windows 7 e Windows 8.
- **Definir UAC para nunca notificar**
  - Desativa o controle de acesso de usuário no Windows Vista, Windows 7 e Windows 8.

Core.1 Windows Procedures.Desktops.Machine Control.Windows Configuration

- **Ocultar uma conta na tela de logon de troca rápida de usuário do Windows**
  - Este script adicionará um valor DWORD com o valor de "suporte ao usuário" e dados 0. Após uma reinicialização, o PC não exibirá mais "suporte ao usuário" na tela de boas-vindas.
- **Cancelar ocultar uma conta na tela de logon de troca rápida de usuário do Windows**
  - Este script adicionará um valor DWORD com o valor de "suporte ao usuário" e dados 0. Após uma reinicialização, o PC não exibirá mais "suporte ao usuário" na tela de boas-vindas.
- **Desativar mostrar arquivos ocultos do sistema operacional**
  - Desativa a opção Mostrar arquivos ocultos do sistema operacional no Windows Explorer.
- **Ativar exibição do conteúdo de pastas do sistema**
  - Ativa a opção Exibir conteúdo de pastas do sistema no Windows Explorer.

- **Ativar ocultar extensões para tipos de arquivos conhecidos**
  - Ativa a opção Ativar ocultar extensões para tipos de arquivos conhecidos no Windows Explorer.
- **Ativar mostrar arquivos e pastas ocultos**
  - Ativa a opção Mostrar arquivos e pastas ocultos no Windows Explorer.
- **Aplicar comprimento mínimo de 8 caracteres para senha do Windows**
  - Força o Windows a rejeitar senhas que não tenham o comprimento mínimo de senha. Previne o uso de senhas comuns em que a segurança é importante. Adiciona um novo valor de REG_BINARY de 'MinPwdLen' e define os dados para o número mínimo de caracteres necessários para que uma senha seja aceita. O exemplo a seguir é 8. Nota: Isto não afeta as senhas existentes, somente as novas ou as modificadas.
- **Suprimir pop-ups de balão para usuário atual do Windows**
  - Suprime todos os pop-ups de balão no Windows para o usuário conectado. Consulte http://msdn.microsoft.com/pt-br/library/ms940877(v=winembedded.5).aspx.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Check Disk

- **Verificar todas as unidades de disco**
  - Usa DISKPART para enumerar todas as partições locais e, em seguida, alimenta essa lista de unidades em CHKDSK para reparar cada volume.
- **Verificar unidade de sistema de disco (agendar na próxima reinicialização)**
  - Executa um comando CHKDSK na unidade do sistema. Os resultados da manutenção são avaliados pelo script de verificação de disco.
- **Verificar unidade de sistema de disco (somente análise)**
  - Executa um comando CHKDSK na unidade do sistema. Os resultados da manutenção são avaliados, uma entrada de log é gravada no log de procedimentos do agente com os resultados e os resultados são recuperados na pasta GetFile do sistema.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Defragmentation

- **Desfragmentar todas as unidades**
  - Usa DISKPART para enumerar todas as partições locais e, em seguida, alimenta essa lista de unidades em DEFRAG para otimizar cada volume. Recupera resultados de DEFRAG de todas as unidades na pasta GetFile do sistema.
- **Desfragmentar unidade de sistema (somente análise)**
  - Realiza uma análise de desfragmentação na unidade do sistema no Windows (geralmente, C:). Os resultados de desfragmentação são gravados no log de procedimentos do agente.
- **Desfragmentar arquivo de páginas e registro**
  - Usa o utilitário PageDefrag do Sysinternals para desfragmentar o arquivo de páginas do sistema e registro, e reiniciar (somente Windows XP).
- **Desfragmentar a unidade do sistema (análise e aviso ao usuário se necessário)**
  - Realiza uma análise de desfragmentação na unidade do sistema no Windows (geralmente, C:). Os resultados de desfragmentação são gravados no log de procedimentos do agente. Se um usuário estiver conectado na máquina, então o procedimento perguntará se ele deseja executar uma desfragmentação completa na unidade e realizará uma se a resposta for sim.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Disk Cleanup

- **Limpeza de disco do Windows**
  - Define as entradas do registro "sageset" para o cleanmgr.exe e então executa o cleanmgr.exe com o parâmetro "sagerun" para limpar automaticamente os arquivos nas

seguintes localizações: Active Setup Temp Folder Content Indexer Cleaner Downloaded Program Files Internet Cache Files Memory Dump Files Old ChkDsk Files Recycle Bin Remote Desktop Cache Files Setup Log Files Temporary Files Temporary Offline Files WebClient and WebPublisher Cache

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Flush DNS

- **Descarregar cache de resolvedor DNS**
  - Descarrega e redefine o conteúdo do cache do resolvedor de cliente DNS ao executar o comando IPCONFIG /FLUSHDNS

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.IE Files Management

- **Limpar os cookies no Internet Explorer**
  - Limpa os cookies do Internet Explorer do usuário atualmente conectado.
- **Limpar os dados do formulário no Internet Explorer**
  - Limpa os dados de formulário do Internet Explorer do usuário atualmente conectado.
- **Limpar o histórico no Internet Explorer**
  - Limpa o histórico do Internet Explorer do usuário atualmente conectado.
- **Limpar as senhas no Internet Explorer**
  - Limpa as senhas do Internet Explorer do usuário atualmente conectado.
- **Limpar arquivos temporários do Internet Explorer**
  - Limpa os arquivos temporários do Internet Explorer do usuário atualmente conectado.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore

- **Criar ponto de restauração semanal do sistema de manutenção da área de trabalho**
  - Usa WMIC para criar um ponto de restauração do sistema chamado de manutenção semanal de desktop. Este procedimento do agente pode ser acionado no início do procedimento de manutenção semanal da estação de trabalho.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.System Restore

- **Criar ponto de restauração do sistema de gerenciamento de correções**
  - Usa WMIC para criar um ponto de restauração do sistema chamado de gerenciamento de correções. Este procedimento do agente pode ser chamado antes de uma implementação de correção através de um procedimento do pré-agente de atualização automática.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.TEMP Files

- **Limpar pasta TEMP do usuário**
  - Exclui todos os arquivos e pastas na pasta %TEMP%, e sob ela, dos usuários conectados que não estão atualmente bloqueados/abertos pelo Windows.

Core.1 Windows Procedures.Desktops.Maintenance.Common Maintenance Tasks.Time Sync

- **Sincronizar hora via SNTP**
  - Define o relógio do Windows para coletar o horário em time.windows.com

Core.1 Windows Procedures.Desktops.Maintenance.Desktop Maintenance

- **Manutenção semanal da estação de trabalho**
  - Executa todas as tarefas de manutenção de desktop semanalmente; agende este script para execução durante o intervalo de manutenção.

Core.1 Windows Procedures.Desktops.Maintenance.Maintenance Notifications

- **Lembrete de manutenção semanal da área de trabalho**
  - Este script foi desenvolvido para execução durante o dia antes da manutenção de correções da área de trabalho. Enviará uma mensagem para um usuário final da área de trabalho, indicando que ele deve sair da máquina no turno da noite.

Core.1 Windows Procedures.Desktops.Software Control.Internet Explorer

- **Definir página inicial do Internet Explorer padrão**
  - Defina a página padrão no Internet Explorer. Basta alterar o site na Etapa 1.

Core.1 Windows Procedures.Desktops.Software Control.Windows Firewall

- **Desativar firewall do Windows**
  - Usa NETSH para desativar o firewall do Windows.

Core.1 Windows Procedures.Servers.Active Directory.AD Replication

- **Realizar uma verificação de replicação de AD usando REPADMIN**
  - Executa uma verificação de replicação em serviços do Active Directory usando o utilitário REPADMIN. Envia resultados por e-mail; você DEVE atualizar o endereço de e-mail para receber os resultados.

Core.1 Windows Procedures.Servers.Exchange.Exchange Best Practices Analyzer.Exchange 2003

- **Servidor ExBPA Report 2003**
  - Desenvolvido para Exchange 2003. Usa o Exchange Best Practice Analyzer para criar um relatório de quaisquer erros. O MS Logparser 2.0 é então usado para analisar os resultados e enviar um e-mail com o relatório final para o endereço de e-mail do administrador que executa/agenda o procedimento do agente. O Exchange Best Practice Analyzer deve ser instalado antes do uso deste procedimento do agente.

Core.1 Windows Procedures.Servers.Exchange.Exchange Best Practices Analyzer.Exchange 2007

- **Servidor ExBPA Report 2007**
  - Desenvolvido para Exchange 2007. Usa o Exchange Best Practice Analyzer para criar um relatório de quaisquer erros. O MS Logparser 2.0 é então usado para analisar os resultados e enviar um e-mail com o relatório final para o endereço de e-mail do administrador que executa/agenda o procedimento do agente. O Exchange Best Practice Analyzer deve ser instalado antes do uso deste procedimento do agente.

Core.1 Windows Procedures.Servers.IIS Server

- **Realizar IISRESET em servidor IIS**
  - Realiza IISReset na máquina.

Core.1 Windows Procedures.Servers.Maintenance

- **Manutenção semanal do servidor**
  - Executa todas as tarefas de manutenção semanal da área de trabalho.

Core.1 Windows Procedures.Servers.Monitoring Remediation.Disk Usage

- **DiskUsage.GetDirTree.C-D-E-F-G-M-N**
  - Retorna o uso de disco em unidades C, D, E, F, G, M e N. Grava os resultados da árvore de uso de disco no log de procedimentos do agente. Unidades não existentes não exibirão quaisquer resultados de uso de disco.

Core.1 Windows Procedures.Servers.Monitoring Remediation.Get Process List

- **Performance.Get Process List**
  - Usa kperfmon.exe para obter a lista do processo, % de CPU e consumo de memória. Esse script pode ser configurado para execução quando os contadores de monitor de desempenho gerarem um alarme. Grava resultados no log de procedimentos do agente.

Core.1 Windows Procedures.Servers.Print Server

- **Limpar filas do spooler de impressão**
  - Interrompe o spooler de impressão, limpa filas e reinicia o spooler de impressão.

Core.1 Windows Procedures.Servers.Service Control Manager

- **Compilar SCM**
  - Recompila o gerenciador de controle de serviço para verificar eventos de SCM que estão conectados ao log do sistema.

Core.1 Windows Procedures.Servers.Terminal Server

- **Terminal Server - Logoff de sessões desconectadas**
  - Efetua logoff de todas as sessões desconectadas de um Terminal Server.
- **Terminal Server - Logoff de sessão X**
  - URL de referência: http://technet2.microsoft.com/windowsserver/en/library/26b3946e-5dbc-4248-9ea4-5adaae45b81f1033.mspx?mfr=true
- **Terminal Server - Log-off da sessão 1**
  - URL de referência: http://technet2.microsoft.com/windowsserver/en/library/26b3946e-5dbc-4248-9ea4-5adaae45b81f1033.mspx?mfr=true
- **Terminal Server - Sessões de consulta**
  - Usa QUERY USER para gerar uma lista de todas as sessões do Terminal Server e grava a lista de informações da sessão no registro de procedimentos do agente.
- **Terminal Server - Reiniciar em 60 segundos**
  - Reinicia um Terminal Server, dando aos usuários conectados 60 segundos para fechar aplicativos e salvar seu trabalho.
- **Terminal Server - Desligar em 60 segundos**
  - Desliga um Terminal Server, dando aos usuários conectados 60 segundos para fechar aplicativos e salvar seu trabalho.

Core.2 Macintosh Procedures

Core.2 Macintosh Procedures.Machine Control.Auditing

- **Coletar informações de HDD, usuário, processo e rede**
  - Coleta algumas informações sobre o Mac. Além disso, funcionará em praticamente qualquer distribuição de Linux quando a Kaseya oferecer suporte a esse processo. Executa DF (Ponto de montagem, informações de espaço em disco) uname -a (Informações de SO) ls /users/ (Informações de usuário) ifconfig (Informações de NIC) netstat (informações de conexão de rede) ps aux (Informações do processo). Os resultados são enviados para /tmp/macinfo.txt e retornados para o servidor Kaseya. Visualizá-los em Auditoria -> Documentos do agente.
- **Recuperar lista de discos e me enviar por e-mail**

- Usa DISKUTIL para relacionar todos os discos Mac OS X, recupera lista de discos para a pasta GetFile dos sistemas e envia um e-mail para o administrador que executou/agendou o procedimento do agente.

Core.2 Macintosh Procedures.Machine Control.Monitoring

- **Verificar status INTELIGENTE de Disk0**
  - Usa DISKUTIL para obter status SMART (Self-Monitoring, Analysis and Reporting Technology) de Disk0 no Mac e envia um e-mail para o administrador que executou/agendou o procedimento se o status SMART estiver com falha.

Core.2 Macintosh Procedures.Machine Control.Networking

- **Vincular Mac a um domínio do Active Directory**
  - Usa DSCONFIGAD para vincular um sistema Mac OS X a um Domínio do Active Directory. Solicita nome de domínio completo do AD, credenciais de "administrador" de domínio do AD e UO de destino.

Core.2 Macintosh Procedures.Machine Control.System

- **Definir configurações de economia de energia do Mac**
  - Define as configurações de economia de energia em Preferências do sistema do Macintosh. Usa PMSET para configurar o perfil do adaptador de energia (ou seja, quando o Mac está conectado à alimentação CA) da seguinte forma: Repouso da tela depois de 45 minutos de inatividade; Repouso do computador depois de 1 hora de inatividade.
- **Atualizar registros de configuração de IP/nome de Mac**
  - Usa CHANGEIP para corrigir alterações de IP/nome em servidores Mac OS X. Solicita o nome antigo e o novo nome com o qual CHANGEIP é usado para atualizar manualmente registros de configuração quando um nome de host ou endereço IP de servidor mudou de forma que serviços afetados não puderam ser devidamente processados; por exemplo, quando o servidor está atrás de um dispositivo NAT e a identidade WAN mudou. No uso característico, esse comando é usado por um administrador para corrigir serviços afetados quando as informações de rede de um servidor mudam. CHANGEIP pode ser acionado antes de a alteração ser aplicada; nesse acionamento, os argumentos consistem nos endereços IP atuais e pendentes do servidor e, opcionalmente, o nome de host existente e novo.
- **Alterar nome do computador Mac**
  - Renomeia Mac com SCUTIL.

Core.2 Macintosh Procedures.Machine ControlSystem Preferences.Energy Saver.Battery Profile

- **Economia de energia - Definição de bateria configurada com redução automática de brilho antes de desativar o repouso de tela**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Redução automática de brilho antes de desativar repouso de tela".
- **Economia de energia - Definição de bateria configurada com redução automática de brilho antes de ativar repouso de tela**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Redução automática de brilho antes de ativar o repouso de tela".
- **Economia de energia - Definição de bateria configurada com repouso de computador em 120 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de computador em 120 minutos".
- **Economia de energia - Definição de bateria configurada com repouso de computador em 15 minutos**

- Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de computador em 15 minutos".

- **Economia de energia - Definição de bateria configurada com repouso de computador em 30 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de computador em 30 minutos".
- **Economia de energia - Definição de bateria configurada com repouso de computador em 45 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de computador em 45 minutos".
- **Economia de energia - Definição de bateria configurada com repouso de computador em 60 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de computador em 60 minutos".
- **Economia de energia - Definição de bateria configurada com repouso de computador em 90 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de computador em 90 minutos".
- **Economia de energia - Definição de bateria configurada com repouso de tela em 120 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de tela em 120 minutos".
- **Economia de energia - Definição de bateria configurada com repouso de tela em 15 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de tela em 15 minutos".
- **Economia de energia - Definição de bateria configurada com repouso de tela em 30 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de tela em 30 minutos".
- **Economia de energia - Definição de bateria configurada com repouso de tela em 45 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de tela em 45 minutos".
- **Economia de energia - Definição de bateria configurada com repouso de tela em 60 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de tela em 60 minutos".
- **Economia de energia - Definição de bateria configurada com repouso de tela em 90 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Repouso de tela em 90 minutos".
- **Economia de energia - Definição de bateria configurada como desativar repouso de discos rígidos quando for possível**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Desativar repouso de discos rígidos quando for possível".
- **Economia de energia - Definição de bateria configurada como ativar repouso de discos rígidos quando possível**

- ➢ Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Ativar repouso de discos rígidos quando for possível".

- **Economia de energia - Definição de bateria configurada como modo de hibernação 0 (ativação da memória)**
  - ➢ Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Modo de hibernação 0 (ativação da memória)".
- **Economia de energia - Definição de bateria configurada como modo de hibernação 25 (ativação de disco)**
  - ➢ Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Modo de hibernação 25 (ativação de disco)".
- **Economia de energia - Definição de bateria configurada como modo de hibernação 3 (ativação de memória ou disco)**
  - ➢ Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Modo de hibernação 3 (ativação de memória ou disco)".
- **Economia de energia - Definição de bateria configurada como desativar leve escurecimento do monitor**
  - ➢ Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Desativar leve escurecimento do monitor".
- **Economia de energia - Definição de bateria configurada como ativar leve escurecimento do monitor**
  - ➢ Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de bateria. O procedimento definirá "Ativar leve escurecimento do monitor"

Core.2 Macintosh Procedures.Machine Control.System Preferences.Energy Saver.Power Adapter Profile

- **Economia de energia - Definição de adaptador de alimentação configurada como redução automática de brilho antes de desativar repouso de tela**
  - ➢ Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Redução automática de brilho antes de desativar repouso de tela".
- **Economia de energia - Definição de adaptador de alimentação configurada como redução automática de brilho antes de ativar repouso de tela**
  - ➢ Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Redução automática de brilho antes de ativar o repouso de tela".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de computador em 120 minutos**
  - ➢ Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de computador em 120 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de computador em 15 minutos**
  - ➢ Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de computador em 15 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de computador em 30 minutos**

- Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de computador em 30 minutos".

- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de computador em 45 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de computador em 45 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de computador em 60 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de computador em 60 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de computador em 90 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de computador em 90 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de tela em 120 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de tela em 120 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de tela em 15 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de tela em 15 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de tela em 30 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de tela em 30 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de tela em 45 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de tela em 45 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de tela em 60 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de tela em 60 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como repouso de tela em 90 minutos**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Repouso de tela em 90 minutos".
- **Economia de energia - Definição de adaptador de alimentação configurada como desativar repouso de discos rígidos quando for possível**

- Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Desativar repouso de discos rígidos quando for possível".

- **Economia de energia - Definição de adaptador de alimentação configurada como ativar repouso de discos rígidos quando for possível**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Ativar repouso de discos rígidos quando for possível".
- **Economia de energia - Definição de adaptador de alimentação configurada como modo de hibernação 0 (ativação da memória)**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Modo de hibernação 0 (ativação da memória)".
- **Economia de energia - Definição de adaptador de alimentação configurada como modo de hibernação 25 (ativação de disco)**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Modo de hibernação 25 (ativação de disco)".
- **Economia de energia - Definição de adaptador de alimentação configurada como modo de hibernação 3 (ativação de memória ou disco)**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Modo de hibernação 3 (ativação de memória ou disco)".
- **Economia de energia - Definição de adaptador de alimentação configurada como desativar ativação para acesso à rede de aeroporto**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Desativar ativação para acesso à rede de aeroporto".
- **Economia de energia - Definição de adaptador de alimentação configurada como ligar ativação para acesso à rede de aeroporto**
  - Usa PMSET para definir configurações de economia de energia em Preferências do sistema Mac para o perfil de adaptador de alimentação. O procedimento definirá "Ligar ativação para acesso à rede de aeroporto".

Core.2 Macintosh Procedures.Machine Control.System Preferences.Security

- **Segurança - Definição geral configurada como desligar desativação de logon automático**
  - Usa DEFAULTS para definir configurações de segurança em Preferências do sistema do Mac como Geral. O procedimento definirá "Ligar desativação de logon automático" e removerá as informações de conta de logon automático existentes.

Core.2 Macintosh Procedures.Machine Control.Utils

- **Reiniciar SO X Dock**
  - Reinicia o Dock Mac.
- **Enviar uma mensagem texto para se comunicar com o OS X**
  - Usa OSASCRIPT e SAY para reproduzir a mensagem inserida no áudio do Mac (ou seja, texto para fala).
- **Tirar uma foto com câmera no OS X**
  - Usa 'isightcapture' da porta do Mac para usar a câmera em qualquer Mac para tirar uma foto.
- **Obter captura de tela da área de trabalho do OS X de usuários atuais**

➢ Realiza uma captura de tela da área de trabalho do Mac OS do usuário conectado no momento. O arquivo de captura de tela é recuperado na pasta Documentos do sistema no servidor.

Core.2 Macintosh Procedures.Maintenance

- **Manutenção semanal de Macintosh**
  - ➢ Realiza várias tarefas de manutenção de roteamento em uma máquina com Macintosh OS X.
- **Limpeza geral de máquina com OS X**
  - ➢ Realiza limpeza do sistema, remove arquivos de log antigos, arquivos "scratch" e "junk", limpa caches do sistema e do usuário, faz a rotatividade de logs de sistema e aplicativos, recria cache DYLD e recria o índice Spotlight.
- **Verificar e reparar volumes de disco do OS X**
  - ➢ Realiza operações de reparo e verificação de disco usando DISKUTIL.
- **Reparar permissões de disco do OS X**
  - ➢ Realiza uma operação de permissões de reparo de disco usando DISKUTIL.

Core.2 Macintosh Procedures.Software Update

- **Atualização de software Mac - Instalar todas as atualizações e alertas, se houver**
  - ➢ Atualização de software Mac - Instala TODAS as atualizações. Se novas atualizações forem instaladas, envia um alerta. Consulte "Atualização de software Mac - Instalar todas as atualizações" em Relatórios -> Logs para obter detalhes. Também são salvos detalhes do agente em Auditoria -> Documentos.
- **Atualização de software Mac - Instalar todas as atualizações e recuperar/registrar resultados em log**
  - ➢ Usa SOFTWAREUPDATE para instalar todas as atualizações de software Mac.
- **Atualização de software Mac - Instalar todas as atualizações e reiniciar depois**
  - ➢ Usa SOFTWAREUPDATE para instalar todas as atualizações de software Mac e reiniciar depois.
- **Atualização de software Mac - Recuperar e me enviar por e-mail a lista de todas as atualizações**
  - ➢ Usa SOFTWAREUPDATE para relacionar todas as atualizações de software Mac em um arquivo e recupera o arquivo e envia a lista para o endereço de e-mail do usuário do VSA que executa/agenda o procedimento.
- **Atualização de software Mac - Fazer download de todas as atualizações e alertas, se houver**
  - ➢ Usa SOFTWAREUPDATE para fazer download de todas as atualizações de software Mac, as relaciona em um arquivo e recupera o arquivo, gerando um alerta se houver atualizações disponíveis.
- **Atualização de software Mac - Fazer download de atualizações recomendadas e alertas, se houver**
  - ➢ Atualizar o software Mac - Download das atualizações recomendadas Se novas atualizações forem obtidas por download, envia um alerta. Consulte "Atualização de software Mac - Fazer download de atualizações recomendadas" em Relatórios -> Logs para obter detalhes. Também são salvos detalhes do agente em Auditoria -> Documentos.
- **Atualização de software Mac: instalar atualizações recomendadas e recuperar/registrar resultados em logs**
  - ➢ Usa SOFTWAREUPDATE para instalar atualizações recomendadas de software Mac.
- **Atualização de software Mac - Recuperar lista de todas as atualizações e alertas, se houver**
  - ➢ Atualização de software Mac - Relacionar TODAS as atualizações. Se novas atualizações forem detectadas, envia um alerta. Consulte "Atualização de software Mac - Relacionar TODAS as atualizações" em Relatórios -> Logs para obter detalhes. Também são salvos detalhes do agente em Auditoria -> Documentos.

Core.3 Linux Procedures

Core.3 Linux Procedures.Machine Control.Audit Info

- **Obter informações atuais de memória**
  - Recupera informações atuais de disponibilidade de memória.
- **Obter versão de Linux e Kernel**
  - Recupera informações atualizadas de Kernel e versão (nome) de Linux.

Core.3 Linux Procedures.Machine Control.DNS

- **Criar arquivo de HOSTS**
  - Este procedimento criará um novo arquivo de hosts com variáveis e informações que você fornecer.
- **Editar servidores DNS**
  - Edita seus servidores DNS.
- **Definir nome de host**
  - Este procedimento configurará o nome de host de seus servidores/estações de trabalho.

Core.3 Linux Procedures.Machine Control.Files/Folder Control

- **Alterar permissões de arquivo/pasta**
  - Ler - Gravar - Executar 4 2 1
- **Alterar propriedade de grupo**
  - chgrp groupName folderName
- **Alterar propriedade**
  - chown userName fileFolderName
- **Excluir qualquer arquivo ou pasta - Perigoso**
  - Este procedimento excluirá qualquer arquivo ou pasta sem pedir permissão.

Core.3 Linux Procedures.Machine Control.Linux Kernel

- **Criar uma imagem initrd**
  - Cria uma imagem initrd do sistema Linux e a nomeia como initrd.image-#version# com base em um valor de versão que você inserir.

Core.3 Linux Procedures.Machine Control.Monitoring

- **Obter arquivo de configuração SNMP**
  - Recupera o arquivo de configuração SNMP usando GET FILE.

Core.3 Linux Procedures.Machine Control.Networking

- **Configuração de cliente DHCP**
  - Adiciona entradas na interface para coleta de servidor DHCP.
- **Configuração de rede (1 interface)**
  - Isso criará um novo arquivo de interface em /etc/networking com novas informações de endereço IP. Isso configurará a rede para somente 1 interface. Assim que o arquivo for criado, o serviço de rede será reiniciado.

Core.3 Linux Procedures.Machine Control.Networking.Get DOMAIN info

- **Consultar todas as informações de domínio**
  - Realiza uma busca completa de DNS de um nome de domínio que você especificar usando DIG com o comando ANY (omnibus - todas as informações de domínio) e recupera o arquivo de log resultante, dig-#domain#-all.log, na pasta GetFile do sistema.

- **Consultar servidor DNS para detalhes de domínio**
  - Realiza uma consulta de DNS de um nome de domínio que você especificar usando DIG e recupera o arquivo de log resultante, dig-#domain#.log, na pasta GetFile do sistema.
- **Consultar servidores DNS de autoridade de um domínio**
  - Realiza uma busca de servidor de nome de autoridade de um nome de domínio que você especificar usando DIG com o comando NS (servidores DNS de autoridade de domínio) e recupera o arquivo de log resultante, dig-#domain#-Auth.log, na pasta GetFile do sistema.
- **Consultar registros de endereço de domínio**
  - Realiza uma busca de DNS de registros de endereço (A) de um nome de domínio que você especificar usando DIG com o comando NS (servidor DNS de autoridade de domínio) e recupera o arquivo de log resultante, dig-#domain#-A.log, na pasta GetFile do sistema.
- **Consultar servidores de e-mail de domínio**
  - Realiza uma busca de DNS de registros de servidores de e-mail/troca de e-mails (MX) de um nome de domínio que você especificar usando DIG com o comando MX (trocas de e-mails de domínio) e recupera o arquivo de log resultante, dig-#domain#-MX.log, na pasta GetFile do sistema.
- **Consultar estatísticas incluindo tempo de ida e volta**
  - Realiza uma consulta de estatísticas (incluindo tempo de ida e volta) de um nome de domínio que você especificar usando DIG e recupera o arquivo de log resultante, dig-#domain#-stats.log, na pasta GetFile do sistema.
- **Consultar TTL de cada registro de recurso**
  - Realiza uma consulta de TTL (Time To Live, Tempo de duração) de DNS de um nome de domínio que você especificar usando DIG e recupera o arquivo de log resultante, dig-#domain#-TTL.log, na pasta GetFile do sistema.

Core.3 Linux Procedures.Machine Control.Networking.Routing

- **Obter rotas**
  - Recupera configuração atual de rotas.
- **Rastrear caminho para domínio/IP**
  - Rastreia HOPS para domínio/endereço IP - Usa GET File para visualizar resultados.

Core.3 Linux Procedures.Machine Control.Reboot/Shutdown

- **Reiniciar Linux**
  - Reinicia o sistema.
- **Desligar Linux**
  - Desliga o sistema Linux.

Core.3 Linux Procedures.Machine Control.Runlevel Control

- **Personalizar nível de execução**
  - Explicação de níveis de execução em Linux http://http://en.wikipedia.org/wiki/Runlevel.
- **Nível de execução 1**
  - O nível de execução 1 é geralmente para comandos muito básicos. Isso é o equivalente a o "modo seguro" usado pelo Windows. Esse nível geralmente é usado somente para avaliar reparos ou manutenção no sistema. Esse é um modo de usuário individual e não permite que outros usuários façam logon na máquina.
- **Nível de execução 2**
  - O nível de execução 2 é usado para iniciar a maioria dos serviços de máquinas. No entanto, ele não inicia o serviço de compartilhamento de arquivos de rede (SMB, NFS). Isso permitirá que vários usuários façam logon na máquina.
- **Nível de execução 3**

- O nível de execução 3 é mais comumente usado por servidores. Isso carrega todos os serviços, exceto o sistema Windows X. Isso significa que o sistema reiniciará para o equivalente de DOS. GUIs (KDE, Gnome) não serão iniciadas. Esse nível permite que vários usuários façam logon na máquina.
- **Nível de execução 4**
  - O nível de execução geralmente é um nível "personalizado". Por padrão, isso iniciará mais alguns serviços do que o nível 3. Geralmente, esse nível é usado somente em circunstâncias especiais.
- **Nível de execução 5**
  - O nível de execução 5 é completo. Ele iniciará quaisquer GUIs, serviços extras de impressão e serviços de terceiros. Vários usuários com recursos completos também são aceitos. Esse nível de execução geralmente é usado por estações de trabalho.

Core.3 Linux Procedures.Machine Control.Services Control

- **Personalizar controle de serviços**
  - Inicia, interrompe e reinicia qualquer serviço no sistema.
- **Reiniciar HTTPD/Apache2**
  - Reinicia seu Web Service HTTPD/Apache2.
- **Reiniciar rede**
  - Reinicia o daemon da rede.
- **Reiniciar NFS**
  - Reinicia o serviço daemon de NFS.
- **Reiniciar Postfix**
  - Reiniciar o servidor de e-mail Postfix.
- **Reiniciar SSH**
  - Reinicia o servidor SSH.
- **Reiniciar ferramentas VMware**
  - Reinicia ferramentas VMware.

Core.3 Linux Procedures.Machine Control.User/Group Control.Groups

- **Criar novo grupo**
  - Usa GROUPADD para criar um novo grupo que você especificar.
- **Excluir grupo**
  - Usa GROUPDEL para excluir um grupo existente que você especificar.

Core.3 Linux Procedures.Machine Control.User/Group Control.Password Control

- **Alterar senha de raiz**
  - Altera senha de raiz no sistema. Por algum motivo, o script retorna status COM FALHA, mas ainda funciona.
- **Alterar senha de usuário**
  - Solicita nome de usuário e redefine.

Core.3 Linux Procedures.Machine Control.User/Group Control.Users

- **Adicionar novo usuário**
  - Adiciona novo usuário Linux.
- **Excluir usuário**
  - Exclui usuário de servidor/máquina.

Core.3 Linux Procedures.Machine Control.Utils

- **Adicionar comandos personalizados**
  - Adiciona vários comandos personalizados com alias ao arquivo /root/.bashrc e então os executa para que esses comandos sejam implementados. Os comandos personalizados são:
    ll = ls –l
    la = ls -A
    l = ls -CF
    *** Estende-se com o acréscimo de mais comandos com alias ***
- **Sincronizar o relógio do sistema**
  - Instala e sincroniza relógio.
- **Atualizar banco de dados de arquivo**
  - Atualiza o banco de dados do sistema de arquivos para uso do comando "locate".

Core.3 Linux Procedures.Maintenance

- **Coletar estatísticas de uso inode**
  - Verifica o uso de inode.
- **Forçar lógica FSCK (File System Check, Verificação do sistema de arquivos) na próxima reinicialização**
  - Força uma FSCK na próxima reinicialização.
- **Obter uso de disco**
  - Gera uma lista de uso de disco usando DF, grava resultados no log de procedimentos do agente e recupera os resultados na pasta GetFile do sistema.
- **Manutenção semanal do Linux**
  - Realiza várias tarefas de manutenção de roteamento em máquinas com Linux, incluindo sincronização de hora, limpeza de repositório apt-get, upgrades/atualizações de pacote, bem como verificações de disco e estatísticas de desempenho.
- **Remover objetos permanentes de Adobe Flash/Macromedia de usuário**
  - Remove objetos permanentes de Adobe Flash e Macromedia de usuário.
- **Remover arquivos temporários de usuário**
  - Remove arquivos temporários (ou seja, *~) da pasta pessoal de usuários atuais.

Core.3 Linux Procedures.Process Control.Get All Processes with PID

  - Recupera todos os processos com ID de processo, usa o recurso GET FILE para recuperar os resultados.
- **Obter árvore de processo**
  - Gera uma ÁRVORE de processos principais e secundários - usa o recurso GET FILE para recuperar os resultados.
- **Eliminar processo**
  - A variável com o PID correto será usada para eliminar o processo geral.
- **Localizar um arquivo**
  - Isso usará a função locate no Kaseya para pesquisar arquivos, conforme especificado, e utilizará o recurso GET FILE para recuperar os resultados.

Core.3 Linux Procedures.Setup/Configs.Backup Servers

- **Backups MySQL com AutoMySQLBackup no Ubuntu 9.10**
  - Instalação do Postfix necessária para instalar o AutoMySQLBackup. O Postfix é necessário http://sourceforge.net/projects/automysqlbackup/ http://www.mysql.com/.
- **Ubuntu Server 9.04 Bacula Bweb GUI**

- Não testado----

Core.3 Linux Procedures.Setup/Configs.CRM Servers.SugarCRM

- A instalação do servidor LAMP completo é necessária antes da instalação do SugarCRM - MySQL, Apached, PHP. Assim que o script for concluído, execute o seguinte: http://Server IP Address/sugarcrm

Core.3 Linux Procedures.Setup/Configs.DNS

- **Configuração de servidor DNS Chrooted**
  - Configura BIND para execução em um ambiente chrooted.

Core.3 Linux Procedures.Setup/Configs.Email Server

- **(2) Configurar servidor de e-mail Postix**
  - Configura o servidor de e-mail Postfix.
- **(2.1) Configurar SMTP-AUTH**
  - Configura autenticação SMTP segura usando SASLAUTHD.
- **(3) Criar os certificados para TLS**
  - Gera certificados TLS.
- **(4) Configurar Postfix para TLS**
  - Configura chaves seguras de TLS para uso do Postfix.
- **(5) Configurar SASLAUTHD para funcionar com Chrooted Postfix**
  - A autenticação será feita por saslauthd. Precisamos fazer algumas alterações para que funcione corretamente. Como o Postfix executa chrooted em /var/spool/postfix, é necessário fazer o seguinte:
- **(6) Instalar Courier-IMAP/Courier-POP3**
  - Instale e configure IMAP e POP3 usando courier - ... e modifique os dois arquivos a seguir; substitua CN=localhost por CN=server1.example.com (você também pode modificar os outros valores, se necessário): vim /etc/courier/imapd.cnf vim /etc/courier/pop3d.cnf
- **(7) Configurar Maildir**
  - Configura Maildir para mensagens de e-mail e caixas de correio de usuário.

Core.3 Linux Procedures.Setup/Configs.FTP Servers

- **Configurar Proftpd**
  - Configura o servidor Proftpd (lembre-se de instalar o software primeiro).

Core.3 Linux Procedures.Setup/Configs.MySQL Server

- **Instalação do servidor MySQL**
  - Instala o servidor MySQL e define senha de raiz.

Core.3 Linux Procedures.Setup/Configs.NFS.NFS Client

- **Instalar e configurar para cliente NFS**
  - Configuração de NFS de máquinas cliente para montagem de unidades como exportado/compartilhado pelo servidor.

Core.3 Linux Procedures.Setup/Configs.NFS.NFS Server

- **Instalar e configurar servidor NFS**
  - Instala e configura o servidor NFS com o diretório HOME e 1 compartilhado opcional com clientes.

Core.3 Linux Procedures.Setup/Configs.Security.AppArmor

- **Desativar AppArmor**
  - AppArmor é uma extensão de segurança (semelhante a SELinux) que deve fornecer mais segurança. Na minha opinião, ela não é necessária para configurar um sistema seguro e geralmente causa mais problemas do que vantagens (imagine o seguinte: depois de ter passado uma semana de trabalho solucionando problemas, pois um serviço não estava funcionando como esperado, você descobre que estava tudo certo, era apenas a AppArmor que estava causando o problema). Portanto, desative-a.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Forward Rules

- **Negar acesso a uma sub-rede específica**
  - Nega acesso a uma sub-rede que você especificar ao adicionar regras de firewall de tabelas ip apropriadas.
- **Tráfego de encaminhamento (DNAT)**
  - Permite encaminhamento DNAT de uma porta TCP específica para o servidor interno. Especifique a interface pública, o endereço público, o endereço de servidor interno e a porta, e o procedimetno adicionará as regras de firewall de tabelas de ip apropriadas.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Global Rules (REJECT, ACCEPT)

- **# Tráfego de encaminhamento (DROP ALL)**
  - Rejeita todo tráfego da cadeia de encaminhamento.
- **# Tráfego de entrada (ALLOW ALL)**
  - Permite todo tráfego de entrada através da cadeia INPUT.
- **# Tráfego de entrada (DROP ALL)**
  - REJEITA todo tráfego de entrada.
- **# Tráfego de saída (ALLOW ALL)**
  - Permite todo tráfego de saída da rede interna.
- **# Tráfego de saída (DROP ALL)**
  - Rejeita todo tráfego interno de saída do firewall.
- **_### NB! - Ativar roteamento - NB! ###_**
  - Permite roteamento e NAT para tabelas de ip. Importante para tráfego a ser processado através do firewall.
- **Não aceitar mensagens de redirecionamento de ICMP**
  - Configura o sistema para não aceitar redirecionamentos de ICMP.
- **Não enviar mensagens de redirecionamento de ICMP**
  - Configura o sistema para não enviar redirecionamentos de ICMP.
- **Liberar mensagens de solicitação eco ICMP enviadas para endereços de transmissão ou multicast.**
  - Configura o sistema para liberar mensagens de solicitação eco ICMP enviadas para endereços de transmissão ou multicast.
- **Liberar pacotes direcionados de origem**
  - Configura o sistema para liberar pacotes direcionados de origem.
- **Ativar registro em logs**
  - Ativa o registro em logs de eventos de firewall de tabelas de ip.
- **Ativar proteção de falsificação de endereço de origem**
  - Ativa a proteção de falsificação de endereço de origem no sistema.
- **Ativar proteção de cookie SYN TCP de inundações de SYN**
  - Ativa proteção de cookie SYN TCP de inundações de SYN no sistema.

- **Descarregar todas as cadeias**
  - Isso descarregará todas as regras de tabelas de ip. É perigoso; esteja ciente do risco!
- **Registrar em log pacotes com endereços de origem impossíveis**
  - Ativa o registro em logs de pacotes com endereços de origem impossíveis no sistema.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Inbound Rules

- **Permitir entrada de porta PERSONALIZADA**
  - Permite que você insira interface, protocolo e porta TCP/UDP que gostaria de adicionar às regras de firewall de tabelas de ip.
- **Permitir entrada de DNS**
  - Permite tráfego de DNS de entrada ao adicionar regras de firewall de tabelas de ip apropriadas. Aplica-se não somente a firewalls atuando como clientes DNS, mas também a firewalls operando com uma função de servidor DNS regular ou de cache.
- **Permitir entrada de FTP**
  - Permite tráfego de FTP de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir entrada de ICMP**
  - Permite tráfego ICMP de entrada ao acrescentar regras de firewall de tabelas de ip apropriadas. Tabelas de ip são configuradas para permitir que o firewall envie solicitações eco ICMP (pings) e, por sua vez, aceitem as respostas eco ICMP esperadas.
- **Permitir entrada de IMAP**
  - Permite tráfego de IMAP de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir entrada de IMAPS**
  - Permite tráfego de IMAPS de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir entrada da Kaseya**
  - Permite tráfego da Kaseya de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir interface de loopback**
  - Permite tráfego de interface de loopback de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir MySQL**
  - Permite tráfego de MySQL de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir que a rede acesse o firewall**
  - eth1 está diretamente conectado a uma rede privada usando endereços IP da rede 192.168.1.0. Presume-se simplesmente que todo tráfego entre essa rede e o firewall é confiável e permitido. Regras adicionais serão necessárias para a interface conectada à Internet, a fim de permitir que somente portas específicas, tipos de conexões e possivelmente até mesmo servidores remotos tenham acesso ao seu firewall e à rede doméstica.
- **Permitir entrada de POP3**
  - Permite tráfego de POP3 de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir entrada de POP3S**
  - Permite tráfego de POP3S de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir entrada de SMTP**

- Permite tráfego de SMTP de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir entrada de SSH**
  - Permite tráfego de SSH de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir tráfego de host local**
  - Permite o tráfego de entrada do endereço de host local ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir entrada de WWW**
  - Pacotes de entrada destinados às portas 80 e 22 são permitidos, realizando assim as primeiras etapas no estabelecimento de uma conexão. Não é necessário especificar essas portas para a parte de retorno, pois são permitidos pacotes de saída para todas as conexões estabelecidas. Conexões iniciadas por pessoas conectadas ao servidor Web serão negadas, pois não são permitidos pacotes NOVOS de conexão de saída.
- **Permitir sessões estabelecidas de entrada**
  - Permite o tráfego de entrada de conexões estabelecidas ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Bloquear endereço IP**
  - Bloqueia um endereço IP que você especifica inserindo sua rede através da interface pública.
- **Bloquear entrada de IRC**
  - Bloqueia o tráfego de IRC de entrada ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Bloquear rede**
  - Bloqueia uma rede inteira de acessar sua rede.
- **Relacionar todas as regras de tabelas de ip**
  - Isso gravará todas as regras de tabelas de ip em /var/tmp/iptables.log e o procedimento GET carregará isso no servidor para análise.
- **Reiniciar tabelas de IP**
  - Reinicia firewall de tabelas de IP.
- **Salvar regras de tabelas de ip**
  - Testado no Ubuntu.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Outbound Rules

- **# Permitir saída da Kaseya**
  - Permite tráfego da Kaseya de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir saída de porta PERSONALIZADA**
  - Permitir que uma porta personalizada de sua rede interna acesse o ambiente externo.
- **Permitir saída de DNS**
  - As seguintes declarações aplicam-se não somente a firewalls atuando como clientes DNS, mas também a firewalls operando com uma função de servidor DNS regular ou de cache.
- **Permitir saída de conexões estabelecidas**
  - Permite todas as conexões estabelecidas com retorno de ACK.
- **Permitir saída de FTP**
  - Permite tráfego de FTP de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir saída de pacotes de ICMP**

- Permite pacotes de ICMP de saída ao adicionar regras de firewall de tabelas de ip apropriadas.

- **Permitir saída de IMAP**
  - Permite tráfego de IMAP de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir saída de IMAPS**
  - Permite tráfego de IMAPS de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir interface de loopback**
  - Permite tráfego de loopback de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir saída de MySQL**
  - Permite tráfego de MySQL de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir saída de POP3**
  - Permite tráfego de POP3 de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir saída de POP3S**
  - Permite tráfego de POP3S de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir saída de SMTP**
  - Permite tráfego de SMTP de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir SSH**
  - Permite tráfego de SSH de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Permitir WWW**
  - Permite tráfego de WWW de saída ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Negar acesso a um endereço IP de saída específico com registro em logs**
  - Nega acesso com registro em logs a um endereço IP de saída que você especificar ao adicionar regras de firewall de tabelas de ip apropriadas.
- **Liberar regras de saída**
  - Libera regras de SAÍDA de tabelas de ip. Perigoso, esteja ciente do risco!
- **Executar todas as regras de SAÍDA**
  - Aplica todas as regras de SAÍDA com capacidade de liberar primeiro, opcionalmente, todas as regras de SAÍDA.

Core.3 Linux Procedures.Setup/Configs.Security.iptables - Linux Firewall.Postrouting Rules

- **Permitir roteamento de rede privada através de firewall**
  - Você observará que a rede privada é uma rede IP roteada não pública. Isso requer conversão de endereços em um roteador com endereço IP público, ou nenhum componente na rede pública será capaz de retornar pacotes para a rede privada. A conversão de endereço é facilmente ativada com tabelas de ip. Os endereços que estão sendo convertidos são a "origem" de sessões; portanto, o modo é chamado de SNAT (Source NAT, NAT de origem):

Core.3 Linux Procedures.Setup/Configs.Security.SELinux

- **Desativar SELinux após reinicialização**

- Isso desativará SELinux por segurança e depois da primeira reinicialização.

- **Desativar SELinux imediatamente**
  - Desativa SELinux do usuário atualmente conectado no nível de execução. Isso não será configurado para ser desativado após a reinicialização.

Core.3 Linux Procedures.Setup/Configs.Shell Control

- **Alterear o Shell padrão**
  - /bin/sh é um symlink para /bin/dash; no entanto, precisamos de /bin/bash, não de /bin/dash.

Core.3 Linux Procedures.Setup/Configs.Web Servers.Apache2

- **Ativar módulos**
  - Módulos Apache (SSL, regravar, suexec, incluir e WebDAV):
- **Instalar Apache2**
  - Usa APT-GET para instalar o servidor Web Apache2, CHKCONFIG para definir como inicialização automática e inicia o daemon Apache.
- **Instalar PHPMyAdmin**
  - Certifique-se de alterar a configuração Apache de forma que phpMyAdmin permita conexões não apenas do host local (ao comentar o stanza<Directory /usr/share/phpMyAdmin/>):

Core.3 Linux Procedures.Setup/Configs.Web Servers.Scripting

- **Instalar PHP5**
  - Instala PHP5 para Apache 2.

Core.3 Linux Procedures.Software Control.Applications

- **Instalar CHKCONFIG**
  - Instala o pacote CHKCONFIG. Este pacote permite que você inicie um pacote de daemon específico na inicialização do sistema.
- **Instalar CHKCONFIG simples**
  - Usa APT-GET para instalar CHKCONFIG.
- **Instalar pacotes necessários comuns**
  - Isso instalará pacotes comumente necessários para o Ubuntu. binutils cpp fetchmail flex gcc libarchive-zip-perl libc6-dev libcompress-zlib-perl libdb4.6-dev libpcre3 libpopt-dev lynx m4 make ncftp nmap openssl perl perl-modules unzip zip zlib1g-dev autoconf automake1.9 libtool bison autotools-dev g++ build-essential.
- **Instalar SNMP**
  - Isso instalará SNMP, que permite que você monitore servidores Linux. Lembre-se de definir sua sequência de comunidade SNMP.
- **Instalar software**
  - Solicita ao usuário o nome do pacote de software que precisa ser instalado e, em seguida, usa APT-GET para instalar esse pacote.
- **Instalar software de lista de imagem**
  - Isso permite que você grave (|) uma lista de software para o comando de instalação apt-get, que instalará todo software ausente na lista. Você precisa criar a lista primeiro. NB (verificar o procedimento da criação da lista de imagem na pasta de atualizações/upgrades de software).
- **Instalar SSH**
  - Instala o servidor SSH para acesso remoto.
- **Instalar VIM**

- Isso instala VIM, um editor de arquivo de texto fácil de usar para Linux.

- **Instalar vim-nox**
  - O programa de vi padrão tem um comportamento estranho no Ubuntu e Debian; para corrigir isso, instalamos vim-nox:
- **Instalar XPDF**
  - Leitor de PDF para Linux.

Core.3 Linux Procedures.Software Control.apt-get

- **Apt-get para limpeza automática**
  - A limpeza automática apt-get remove somente arquivos de pacote que não podem mais ser obtidos por download.
- **Limpar repositório apt-get**
  - Remove tudo, exceto arquivos de bloqueio de /var/cache/apt/archives/ e /var/cache/apt/archives/partial/. Portanto, se você precisar instalar um APT de pacote, deverá recuperá-lo novamente.
- **Instalar software**
  - Solicita ao usuário o nome do pacote de software que precisa ser instalado e, em seguida, usa APT-GET para instalar esse pacote.
- **Remover software**
  - Remove o pacote como solicitado pelo procedimento.

Core.3 Linux Procedures.Software Control.DNS

- **Instalar Bind9**
  - Servidor DNS para Linux.

Core.3 Linux Procedures.Software Control.Email Servers

- **Fazer download do Zimbra Email**
  - Isso fará download do pacote de colaboração de e-mail Zimbra para Linux.

Core.3 Linux Procedures.Software Control.File Server

- **Instalar cota**
  - Isso instalará o aplicativo de cota necessário para controle de cotas em pastas específicas. É altamente recomendado que você edite seu arquivo /etc/fstab manualmente, pois isso pode interromper seu servidor e não montará qualquer sistema de arquivos. Aqui está um exemplo de um fstab de trabalho com cota ativada:

```
# <file system> <mount point>   <type>  <options>      <dump>  <pass>
proc           /proc          proc    nodev,noexec,nosuid 0      0
/dev/mapper/server1-root /             ext4
errors=remount-ro,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0
1
# /boot was on /dev/sda1 during installation
UUID=a8f37dcf-5836-485c-a451-3ae2f0f47720 /boot         ext2    defaults
0      2
/dev/mapper/server1-swap_1 none          swap    sw            0      0
/dev/fd0       /media/floppy0  auto    rw,user,noauto,exec,utf8 0      0
```

- **Definir ativação de cota**
  - Ativar gerenciamento de cota paras servidores de arquivos.

Core.3 Linux Procedures.Software Control.FTP Servers

- **Instalar Proftpd**
  - Isso instalará o servidor Proftp para Linux.

Core.3 Linux Procedures.Software Control.iptables (Firewall)

- **Instalar tabelas de ip**
  - Usa APT-GET para instalar firewall de tabelas de ip.

Core.3 Linux Procedures.Software Control.Management Software

- **Fazer download do Webmin**
  - Webmin é uma GUI usada para o gerenciamento total de Linux usando seu navegador da Web.

Core.3 Linux Procedures.Software Control.Repository's

- **Ativar repositório multiverso**
  - Isso adicionará as origens ao arquivo source.list. Isso não recriará o arquivo.
- **Ativar repositório universo**
  - Esse procedimento adicionará esse repositório ao arquivo de origens. Isso não recriará o arquivo.
- **Atualizar repositório**
  - Atualiza todos os pacotes. Execute isso depois de adicionar o repositório.

Core.3 Linux Procedures.Software Control.System

- **Instalar daemon NTP**
  - É uma boa idea sincronizar o relógio do sistema com um servidor NTP (network time protocol, protocolo de hora de rede) pela Internet. Basta executar.

Core.3 Linux Procedures.Software Control.Updates/Upgrades

- **Criar lista de imagem de software instalado**
  - Cria lista de imagem de software instalado.
- **Atualização total do sistema**
  - Atualiza todos os pacotes do sistema.
- **Realizar upgrade de pacotes**
  - Use esse procedimento para realizar upgrade de pacotes na mesma distribuição.
- **Realizar upgrade para nova versão**
  - Realiza upgrade de seu Linux Distro para a versão mais recente disponível. Você verá uma solicitação de reinicialização na área de trabalho quando concluir.
- **Atualizações/upgrades de pacote Linux**
  - Realiza uma atualização total do sistema e upgrade de todos os pacotes instalados.

Core.4 Other Tools and Utility Procedures

Core.4 Other Tools and Utility Procedures.AntiVirus

- **Teste de vírus EICAR**
  - Cria um arquivo no diretório de trabalho do agente que contém o padrão de vírus de teste EICAR. Esse procedimento do agente pode ser usado para verificar se qualquer software antivírus está funcionando em uma máquina. NOTA: Isso não é um vírus real e não apresenta potencial de risco. Para obter mais informações, consulte http://eicar.org.
- **Executar uma varredura-limpeza completa da ferramenta de remoção de software mal-intencionado**
  - Usa MRT (Microsoft Malicious Software Removal Tool) para realizar uma varredura e limpeza completas. Os resultados da operação são registrados em logs em um arquivo MRT.LOG e no log de procedimentos do agente. O arquivo de log é recuperado na pasta GetFile do sistema.

Core.4 Other Tools and Utility Procedures.AntiVirus.Defender

- **Windows Defender - rastreamento completo do sistema**
  - Executa um rastreamento completo do sistema com Windows Defender.
- **Windows Defender - rastreamento rápido do sistema**
  - Executa um rastreamento rápido do sistema com Windows Defender.
- **Windows Defender - atualização de assinatura**
  - Executar uma atualização de assinatura do Windows Defender.

Core.4 Other Tools and Utility Procedures.AutoAdminLogon

- **Desativar AutoAdminLogon**
  - Desativa qualquer configuração AutoAdminLogon ativada anteriormente em uma máquina com Windows.
- **Ativar AutoAdminLogon com AUTOLOGON**
  - Ativa AutoAdminLogon com criptografia de senha segura usando o utilitário SysInternals AutoLogon. Este procedimento do agente funciona somente em versões de 32 bits do Windows XP ou versão posterior.
- **Ativar AutoAdminLogon com método de texto simples**
  - Solicita o nome de usuário e senha a serem usados para AutoAdminLogin; em seguida, ativa a configuração de AutoAdminLogon de texto simples em uma máquina com Windows usando essas credenciais fornecidas.

Core.4 Other Tools and Utility Procedures.Kaseya Agent Management

- **Agente - Forçar a entrada**
  - Este é o procedimento mais curto do mundo. Este procedimento não tem nenhuma etapa. Sua única função é a de forçar o Agente a entrar no KServer. Utilize Forçar entrada para determinar se o Agente está ou não on-line.
- **Agente - Remover Kaseya do menu Iniciar e Adicionar/Remover programas**
  - Remove a pasta Agente do menu Iniciar. Oculta o ícone da bandeja do sistema (K azul) ao desativar o menu Agente (guia Agente – menu Agente). Execute este script nas máquinas em que não deseja mais conceder a habilidade para desinstalar, sair ou parar o Agente.
- **Agente - Redefinir cache de auditoria**
  - Exclui o arquivo de resultados de auditoria em cache salvo pelo Agente. Execute este script para redefinir todos os resultados do aplicativo de uma auditoria e reiniciar.
- **Agente - Encerrar sessões de controle remoto**
  - Esse script encerra todas as sessões de controle remoto compatíveis com o Kaseya na função de controle remoto do VSA (K-VNC, WinVNC, Terminal Services, FTP, RAdmin e pcAnyWhere).
- **VNC - Ocultar ícone da bandeja do sistema**
  - Desativa o ícone da bandeja do sistema do VNC em máquinas com Windows quando o serviço VNC estiver em execução.
- **VNC - Definir limite de tempo ocioso como 0 (Nunca ultrapassar o limite de tempo)**
  - Define o limite de tempo ocioso do VNC como 0, a fim de que uma sessão de RC do VNC ocioso não seja desconectada. Útil ao realizar operações remotas em máquinas que demoram muito para concluir, bem como quando você não deseja que a sessão de VNC atinja automaticamente o limite de tempo depois de 1 hora (padrão) de inatividade.
- **VNC - Ativar o protetor de tela no remoto**
  - Ativa papel de parede ao controlar remotamente um sistema com ícone de desativar VNC para controle remoto totalmente em segundo plano para um agente.
- **VNC - Remover o RealVNC do menu Iniciar**

- Remove a entrada RealVNC do menu Iniciar.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Ping Check

- **Ping do endereço IP 1**
  - Este procedimento efetua o ping do endereço IP para obter os resultados que podem ser usados em outro procedimento. Isto também pode ser uma porta ou qualquer outro dispositivo.
- **Ping do endereço IP 2**
  - Este procedimento irá testar a variável do Ping do endereço IP, para verificar se o endereço pode obter o ping sem a perda do pacote. Se houver a perda do pacote, o sistema irá enviar um e-mail com os resultados do ping. Se não houver perda do pacote, ele irá registrar um resultado Tudo OK.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Port Check

- **Monitoramento da porta 1**
  - Parte 1 de 2: Monitora um porta em um host ou endereço IP, e envia um e-mail quando a porta falha em responder. Edite a Eatapa 1 com o nome do host ou endereço IP, edite a Etapa 2 para inserir o número da porta que deseja monitorar, e edite a Eatapa 3 para especificar os endereços de e-mail (múltiplos endereços separados por vírgula) para enviar um alerta quando a porta falha em responder. Edite o prodimento Monitor da porta 2 para modificar o assunto e corpo do e-mail.
- **Monitoramento da porta 2**
  - NÃO agendar este procedimento. É um procedimento secundário denominado Port Monitor 1. Agende o Port Monitor 1 para ser executado em uma máquina onde você deseja monitorar uma porta, host ou Endereço IP.

Core.4 Other Tools and Utility Procedures.Managed Services.Monitoring.Web Check

- **Verificação Web 1**
  - O procedimento extrai a saída da página da Web configurada como a variável siteURL. O script da verificação Web 2 verificará se o conteúdo esperado existe na saída. Você deve configurar a variável siteURL e a sequência de busca do arquivo de teste na verificação Web 2 para personalizar esse procedimento. Essa amostra verifica www.google.com/index.html quanto à palavra "google".
- **Verificação Web 2**
  - A Verificação Web 2 verifica se o conteúdo esperado existe na saída da solicitação de URL. Você deve alterar o comando do arquivo de teste para o conteúdo que seria encontrado quando o URL testado estiver funcional. Nessa amostra, verificamos se a palavra "google" existe na página inicial do Google.

Core.4 Other Tools and Utility Procedures.Managed Services.Policy Management

- **Atualização de política do grupo Windows (GPUPDATE /FORCE)**
  - Recarrega a Política de grupos nas máquinas com Windows.

Core.4 Other Tools and Utility Procedures.Managed Services.Server Management.Services Remediation

- **Iniciar serviço (W32Time)**
  - Esse procedimento reinicia o serviço de hora do Windows. Esse é um procedimento de amostra que demonstra como iniciar um serviço usando procedimentos do agente Kaseya.
- **Interromper serviço (W32Time)**
  - Esse procedimento interrompe o serviço de hora do Windows. Esse é um procedimento de amostra que demonstra como interromper um serviço usando procedimentos do agente Kaseya.

Core.4 Other Tools and Utility Procedures.Managed Services.Server Management.Terminal Services

- **Alterar porta de escuta de RDP de serviços de terminal**
  - Esse procedimento altera a porta de RDP de serviços de terminal padrão de 3389 para uma nova porta de sua escolha.

Core.4 Other Tools and Utility Procedures.Managed Services.System Management

- **Fazer download do SysInternals Process Explorer**
  - Esta amostra demonstra como fazer download de arquivos de origens remotas usando o comando Get URL do procedimento do agente. Basta especificar tanto o URL para fazer download quanto o local de destino. Nesta amostra, fazemos download diretamente do site do fornecedor; no entanto, um método conhecido de distribuir seus arquivos é armazená-los em um site ou ftp acessível para o público (armazenamento em nuvem) usando esse método para obtê-los por download para seus endpoints. Essa amostra simplesmente faz download do arquivo; no entanto, você pode estender a funcionalidade para instalar ou executar arquivos usando o comando de execução de Shell nos procedimentos do agente. Além disso, observe que nesse script usamos uma variável para o diretório temp do agente. Consulte **Caminho de diretório de trabalho do agente** em **Como usar variáveis** *(http://help.kaseya.com/webhelp/PTB/VSA/7000000/index.asp#2855.htm)* na ajuda on-line do VSA.
- **Enviar mensagem se conectado**
  - Este procedimento irá enviar uma mensagem para todos seus usuários informando da necessidade de manutenção. Em um sistema, você pode utilizar a guia Controle remoto para enviar uma mensagem, mas não há forma de mandar uma mensagem se eles estiverem conectados.

Core.4 Other Tools and Utility Procedures.Operational Communications

- **Copiar mensagens OpComm**
  - Copia todos os arquivos de mensagem OpComm mais recentes do servidor para a máquina de destino.
- **Obter nome de usuário e então dar as boas-vindas**
  - Recupera o usuário atualmente conectado de uma visualização do SQL e então envia uma mensagem de boas-vindas de nosso serviço de suporte de TI para esse usuário. Se nenhum usuário estiver conectado, o procedimento do agente será reagendado para execução novamente em 10 minutos.
- **OpComm-ActionRequired**
  - Exibe a mensagem ActionRequired para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.
- **OpComm-Backup**
  - Exibe a mensagem Backup OpComm para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.
- **OpComm-Emergency**
  - Exibe a mensagem Emergency OpComm para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.

- **OpCommm-MachineAudit**
  - Exibe a mensagem MachineAudit OpComm para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.
- **OpComm-MaintSchedule**
  - Exibe a mensagem MaintSchedule OpComm para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.
- **OpComm-NetworkDowntime**
  - Exibe a mensagem NetworkDowntime OpComm para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.
- **OpComm-PatchUpdate**
  - Exibe a mensagem PatchUpdate OpComm para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.
- **OpComm-RegularMaintenance**
  - Exibe a mensagem RegularMaintenance OpComm para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.
- **OpComm-VirusScan**
  - Exibe a mensagem VirusScan OpComm para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.
- **OpComm-VirusThreat**
  - Exibe a mensagem VirusThreat OpComm para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.
- **OpComm-Welcome**
  - Exibe a mensagem Welcome OpComm para o usuário conectado. Mensagens OpComm são para comunicação de atividades operacionais padrão, notificações e lembretes. A pasta de mensagens OpComm pode ser personalizada e estendida para suporte a outras formas

de comunicações de usuários finais. Esses arquivos estão localizados na pasta Kaseya\WebPages\ManagedFiles\VSASharedFiles\OpComm no servidor Kaseya.

Core.4 Other Tools and Utility Procedures.Patch Management

- **Verificação de status WinAutoUpdate**
  - Verifica o último status conhecido da atualização automática do Windows com base na varredura de correção mais recente e executa a opção "WinAutoUpdate ativada", se ativada, ou "WinAutoUpdate desativada", se desativada. Usado para criar Visualizações mostrando máquinas com a atualização automática do Windows ativada ou desativada.
- **WinAutoUpdate desativada**
  - NÃO EXECUTAR/AGENDAR ESTE PROCEDIMENTO. Ele é chamado de "Verificação de status WinAutoUpdate" se a atualização automática do Windows estiver desativada em uma máquina.
- **WinAutoUpdate ativada**
  - NÃO EXECUTAR/AGENDAR ESTE PROCEDIMENTO. Ele é chamado de "Verificação de status WinAutoUpdate" se a atualização automática do Windows estiver ativada em uma máquina.
- **Criar compartilhamento de repositório**
  - Cria a pasta local de origem de arquivo e compartilhamento de rede para atuar como o repositório para correções do Windows obtidas por download da Internet via o Patch Management.
- **Pré-aviso de correção**
  - Envia uma mensagem para o usuário conectado de que atualizações de segurança e correções estão prestes a ser instaladas na máquina. Desenvolvido para ser usado como um pré-procedimento para atualizações automáticas de correções.
- **Reinicialização da correção**
  - Em estações de trabalho com Windows, o procedimento solicita que um usuário conectado reinicie devido a atualizações/correções de segurança instaladas. Se o usuário responder Sim, então ele será notificado de que o sistema será reiniciado em um minuto, deverá salvar o trabalho e fechar seus aplicativos. Se o usuário responder Não, então ele agendará novamente a execução em 60 minutos. Se nenhum usuário estiver conectado na estação de trabalho, então o sistema será reiniciado. Se a máquina for um servidor e o endereço de e-mail de reinicialização de correção estiver configurado, então o procedimento enviará um e-mail para esse endereço de e-mail, indicando que a máquina precisa de atenção (uma reinicialização).

Core.4 Other Tools and Utility Procedures.Patch Management.Suspend Alarms After Patch

- **Pós-correção-Cancelar suspensão de alarmes**
  - Retoma alarmes relacionados a monitoramento. Desenvolvido para ser usado como um pós-procedimento para atualizações automáticas de correções quando a máquina for reiniciada imediatamente depois da correção.
- **Suspender alarmes por 10 minutos**
  - Suspende alarmes relacionados a monitoramento por 10 minutos. Desenvolvido para execução como um pós-procedimento para atualizações automáticas de correções quando a reinicialização ocorre automaticamente depois da correção.
- **Suspender alarmes por 10 minutos - Recorrente**
  - Suspende alarmes relacionados a monitoramento por 10 minutos e agenda novamente a execução em 5 minutos; portanto, não há lacunas possíveis no intervalo de alarme suspenso. Desenvolvido para execução como um pós-procedimento para atualizações automáticas de correções quando a reinicialização não ocorrer imediatamente.
- **Suspender alarmes por 120 minutos**

- Suspende alarmes relacionados a monitoramento por 120 minutos. Desenvolvido para execução como um pós-procedimento para atualizações automáticas de correções quando a reinicialização não ocorre automaticamente depois da correção.

Core.4 Other Tools and Utility Procedures.Run Now System Scripts

- **Executar agora auditoria base**
  - Executa o procedimento "auditoria base" do agente do sistema.
- **Executar agora desativação de atualização automática do Windows**
  - Executa o procedimento "Desativar atualização automática do Windows" do agente do sistema.
- **Executar agora auditoria mais recente**
  - Executa o procedimento "auditoria mais recente" do agente do sistema.
- **Executar agora varredura de correção**
  - Executa o procedimento "varredura de correções" do agente do sistema.
- **Executar agora auditoria de funções do servidor**
  - Executa o script do sistema LUA por parte do cliente para realizar uma auditoria de funções do servidor.
- **Executar agora informações do sistema**
  - Executa o procedimento "informações do sistema" do agente do sistema.
- **Executar agora atualização de listas por varredura**
  - Executa o procedimento "Atualizar listas por varredura" do agente do sistema.
- **Executar agora desinstalação do agente (Retém dados do agente)**
  - Executa o procedimento "Desinstalar agente" do agente do sistema. Depois que o agente for desinstalado, o sistema reterá dados desse agente no sistema até que seja excluído manualmente.
- **Executar agora redefinição de atualização automática do Windows**
  - Executa o procedimento "Redefinir atualização automática do Windows" do agente do sistema.

Conjuntos de monitores

Backup

- **Backup - Backup Exec Continuous Protection Services - {Severity3}**
  - Monitora serviços de proteção contínua de execução de backup em servidores de execução de backup. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Backup - Backup Exec DLO Agent Services - {Severity3}**
  - Monitora serviços de agente DLO de execução de backup em servidores de execução de backup. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Backup - Backup Exec Services - {Severity3}**
  - Monitora serviços de execução de backup em servidores de execução de backup. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Backup - Backup Exec System Recovery Service - {Severity3}**

- Monitora serviço de recuperação de execução de backup em servidores de execução de backup. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

- **Backup - BrightStor ARCServe Backup Services - {Severity3}**
  - Monitora serviços de backup do BrightStor ARCServe em servidores de backup BrightStor ARCServe. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Banco de dados

- **Database - SQL Server (All Instances) Services - {Severity3}**
  - Monitora serviços SQL Server em servidores SQL Server usando o serviço MSSQL* de caractere curinga. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Database - SQL Server (Default Instance) - {Severity0}**
  - Coleta contadores de desempenho do servidor SQL (instância padrão) em servidores SQL. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Database - SQL Server (Default Instance) Performance - {Severity2}**
  - Monitora desempenho do servidor SQL (instância padrão) em servidores SQL. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Database - SQL Server (Default Instance) Services - {Severity3}**
  - Monitora serviços do servidor SQL (instância padrão) em servidores SQL. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Database - SQL Server 2005 Optional Services - {Severity3}**
  - Monitora serviços opcionais de SQL Server 2005 em servidores SQL Server 2005. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Database - SQL Server 2005 Services - {Severity3}**
  - Monitora serviços de SQL Server 2005 em servidores SQL Server 2005. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Database - SQL Server 2008 Optional Services - {Severity3}**
  - Monitora serviços opcionais de SQL Server 2008 em servidores SQL Server 2008. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Database - SQL Server 2008 Services - {Severity3}**
  - Monitora serviços de SQL Server 2008 em servidores SQL Server 2008. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

E-mail

- **Email - Blackberry Server Performance - {Severity2}**
  - Monitora desempenho de Blackberry Server em servidores Blackberry. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Email - BlackBerry Server Services - {Severity3}**
  - Monitora serviços dos servidores Blackberry Server em servidores Blackberry. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

- **Email - Exchange 2003 Services - {Severity3}**
  - Monitora serviços do Exchange 2003 em servidores Exchange 2003. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange 2007 Services - {Severity3}**
  - Monitora serviços do Exchange 2007 em servidores Exchange 2007. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange 2010 Edge Transport Queues - {Severity0}**
  - Coleta contadores de desempenho de filas de transporte de borda do Exchange 2010 em servidores Exchange 2010. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity2}**
  - Monitora contadores de desempenho de filas de transporte de borda do Exchange 2010 em servidores Exchange 2010. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Email - Exchange 2010 Edge Transport Queues Performance - {Severity3}**
  - Monitora contadores de desempenho de filas de transporte de borda do Exchange 2010 em servidores Exchange 2010. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange 2010 Services - {Severity3}**
  - Monitora serviços do Exchange 2010 em máquinas Exchange 2010. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange Client Active Logons - {Severity0}**
  - Coleta contador de desempenho de logons ativos de cliente Exchange em servidores Exchange. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Email - Exchange IMAP4 Service - {Severity3}**
  - Monitora serviço IMAP4 do Exchange em servidores Exchange. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange POP3 Service - {Severity3}**
  - Monitora serviço POP3 do Exchange em servidores Exchange. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange Server (Core) Performance - {Severity2}**
  - Monitora desempenho de servidor Exchange em servidores Exchange. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Email - Exchange Server (Core) Services - {Severity3}**
  - Monitora serviços do servidor Exchange (Core) em máquinas com Exchange Server (Core). Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Email - Exchange Server (Core) Store and Database - {Severity0}**
  - Coleta contadores de desempenho de banco de dados e loja do servidor Exchange em servidores Exchange. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Email - SMTP Queue Performance - {Severity3}**

- Monitora o desempenho de fila SMTP em servidores SMTP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

- **Email - SMTP Server Service - {Severity3}**
    - Monitora o serviço de servidor SMTP em servidores SMTP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Arquivo/impressão

- **File / Print - DFS Service - {Severity3}**
    - Monitora o serviço DFS em máquinas DFS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **File / Print - DFSR Service - {Severity3}**
    - Monitora o serviço DFSR em máquinas DFSR. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **File / Print - NTFRS Service - {Severity3}**
    - Monitora o serviço NTFRS em máquinas NTFRS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **File / Print - Print Queue Job Errors Performance - {Severity1}**
    - Monitora o desempenho de erros de trabalho da fila de impressão em servidores de arquivo e impressão. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **File / Print - Spooler Service - {Severity3}**
    - Monitora o serviço de spooler em serviços de arquivo e impressão. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Infraestrutura de rede

- **Network Infrastructure - Active Directory Domain Controller Services - {Severity3}**
    - Monitora serviços do controlador de domínio do Active Directory em controladores de domínio do Active Directory. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Network Infrastructure - AD Domain Controller Performance - {Severity2}**
    - Monitora desempenho de controlador de domínio do AD em controladores de domínio do Active Directory. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Network Infrastructure - DHCP Server Performance - {Severity2}**
    - Monitora desempenho de servidor DHCP em servidores DHCP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Network Infrastructure - DHCP Server Service - {Severity3}**
    - Monitora o serviço do servidor DHCP em servidores DHCP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Network Infrastructure - DNS Server Performance - {Severity2}**
    - Monitora desempenho de servidor DNS em servidores DNS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Network Infrastructure - DNS Server Service - {Severity3}**

- Monitora o serviço de servidor DNS em servidores DNS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

- **Network Infrastructure - WINS Server Service - {Severity3}**
  - Monitora o serviço do servidor WINS em servidores WINS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Disk Space.Disk Space

- **Windows (Core) - Free Disk Space on Any Drive Below 1GB - {Severity2}**
  - Monitora o espaço livre em disco em qualquer unidade abaixo de 1GB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Windows (Core) - Free Disk Space on Any Drive Below 2GB - {Severity1}**
  - Monitora o espaço livre em disco em qualquer unidade abaixo de 2GB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Disk Space on Any Drive Below 750MB - {Severity3}**
  - Monitora o espaço livre em disco em qualquer unidade abaixo de 750 MB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Disk Space on Drive C - {Severity3}**
  - Monitora o espaço livre em disco na unidade C em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Disk Space on Drive C Below 1GB - {Severity2}**
  - Monitora o espaço livre em disco na unidade C abaixo de 1GB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Windows (Core) - Free Disk Space on Drive C Below 750MB - {Severity3}**
  - Monitora o espaço livre em disco na unidade C abaixo de 750 MB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Disk Space on Drive D - {Severity3}**
  - Monitora o espaço livre em disco na unidade D em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Disk Space on Drive E - {Severity3}**
  - Monitora o espaço livre em disco na unidade E em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Disk Space on Drive F - {Severity3}**
  - Monitora o espaço livre em disco na unidade F em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Disk Space on Drive G - {Severity3}**
  - Monitora o espaço livre em disco na unidade G em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows (Core) - Free Space on C Drive Below 15 Percent - {Severity1}**

- Monitora o espaço livre na unidade C abaixo de 15% em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.

- **Windows (Core) - Free Space on C Drive Below 2GB - {Severity1}**
  - Monitora o espaço livre em disco na unidade C abaixo de 2GB em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Space on D Drive Below 15 Percent - {Severity1}**
  - Monitora o espaço livre na unidade D abaixo de 15% em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Space on E Drive Below 15 Percent - {Severity1}**
  - Monitora o espaço livre na unidade E abaixo de 15% em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Space on F Drive Below 15 Percent - {Severity1}**
  - Monitora o espaço livre na unidade F abaixo de 15% em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows (Core) - Free Space on G Drive Below 15 Percent - {Severity1}**
  - Monitora o espaço livre na unidade G abaixo de 15% em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.

Windows (Core)

- **Windows (Core) - All Automatic Services - {Severity0}**
  - Coleta status de serviço de todos os serviços automáticos em máquinas com Windows. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Windows (Core) - CPU and Memory - {Severity0}**
  - Coleta contadores de desempenho de CPU e memória em máquinas com Windows. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Windows (Core) - Machine Health - {Severity0}**
  - Coleta contadores de desempenho de integridade de máquina em máquinas com Windows. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Windows (Core) - Processor and Memory Performance - {Severity2}**
  - Monitora o desempenho do processador e memória em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Windows (Core) - TCPv4 Connections Performance - {Severity2}**
  - Monitora o desempenho de conexões TCPv4 em máquinas com Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.

Windows Servers

- **Windows Server (Core) - Cluster Services - {Severity3}**
  - Monitora serviços de cluster em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows Server (Core) - Disk Time and Queue Length Performance - {Severity2}**

- Monitora o desempenho de comprimento de fila e tempo de disco em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.
- **Windows Server (Core) - Drive C Performance - {Severity1}**
  - Monitora o desempenho da unidade C em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows Server (Core) - General System Performance - {Severity1}**
  - Monitora o desempenho geral do sistema em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows Server (Core) - Server Reboots - {Severity1}**
  - Monitora reinicializações de servidor em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows Server (Core) - Standard Services - {Severity3}**
  - Monitora serviços padrão em servidores Windows. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows Server 2003 - Standard Services - {Severity3}**
  - Monitora serviços padrão em máquinas com Windows Server 2003. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows Server 2008 - Standard Services - {Severity3}**
  - Monitora serviços padrão em máquinas com Windows Server 2008. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Windows Server 2012 - Standard Services - {Severity3}**
  - Descrição: Monitora serviços padrão em máquinas com Windows Server 2012. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Estações de trabalho com Windows

- **Windows 7 - Standard Services - {Severity1}**
  - Monitora serviços padrão em máquinas com Windows 7. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows 8 - Standard Services - {Severity1}**
  - Monitora serviços padrão em máquinas com Windows 8. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows Vista - Standard Services - {Severity1}**
  - Monitora serviços padrão em máquinas com Windows Vista. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.
- **Windows XP - Standard Services - {Severity1}**
  - Monitora serviços padrão em máquinas com Windows XP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 1.

Acesso remoto

- **Remote Access - Citrix Licensing Service - {Severity3}**
  - Monitora serviço de licenciamento Citrix em servidores Citrix. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Citrix Licensing WMI Service - {Severity3}**
  - Monitora serviço WMI de licenciamento Citrix em servidores Citrix. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Citrix MetaFrame Services - {Severity3}**
  - Monitora serviços Citrix MetaFrame em servidores Citrix. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Citrix Server Services - {Severity3}**
  - Monitora serviços do servidor Citrix em servidores Citrix. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Citrix Virtual Memory Optimization Service - {Severity3}**
  - Monitora serviço de otimização de memória virtual Citrix em servidores Citrix. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Terminal Server Services - {Severity3}**
  - Monitora serviços do Terminal Server em servidores de Terminal. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Remote Access - Terminal Server Session Performance - {Severity2}**
  - Monitora desempenho de sessão do Terminal Server em servidores de Terminal. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 2.

Segurança/antivírus

- **AV - AVG Tech AVG Services - {Severity3}**
  - Monitora serviços AVG da AVG Tech em máquinas AVG da AVG Tech. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - McAfee Enterprise Services - {Severity3}**
  - Monitora serviços McAfee Enterprise em máquinas com McAfee Enterprise. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Microsoft SE-FEP Services {Severity3}**
  - Monitora Microsoft SE-FEP Services em máquinas com Microsoft SE-FEP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Sophos Antivirus Services - {Severity3}**
  - Monitora serviços da Sophos Antivirus em máquinas com Sophos Antivirus. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Symantec Antivirus Services - {Severity3}**

- Monitora serviços da Symantec Antivirus em máquinas com Symantec Antivirus. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

- **AV - Symantec Endpoint Protection Services - {Severity3}**
  - Monitora serviços de proteção endpoint da Symantec em máquinas com Symantec Endpoint Protection. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Trend Micro Client Server Security Services - {Severity3}**
  - Monitora serviços de segurança de servidor cliente da Trend Micro em máquinas com Trend Micro Client Server Security. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **AV - Trend Micro OfficeScan Services - {Severity3}**
  - Monitora serviços Trend Micro OfficeScan em máquinas com Trend Micro OfficeScan. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Sistemas Web

- **Web Systems - FTP Server Service - {Severity3}**
  - Monitora o serviço do servidor FTP em servidores FTP. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Web Systems - IIS Performance - {Severity3}**
  - Monitora o desempenho de IIS em servidores IIS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Web Systems - IIS Server - {Severity0}**
  - Coleta contadores de desempenho de servidor IIS em servidores IIS. Usado somente para fins de geração de relatórios e exibição de logs de monitores.
- **Web Systems - IIS Server Services - {Severity3}**
  - Monitora serviços de servidor IIS em servidores IIS. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.
- **Web Systems - SharePoint Server Services - {Severity3}**
  - Monitora serviços de servidor SharePoint em servidores SharePoint. Usado para fins de alertas, geração de relatórios e exibição de log de monitores. Os alarmes são considerados de gravidade 3.

Conjunto de eventos

Segurança/antivírus

- **zz[SYS] AV - McAfee Anti-Virus (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do McAfee Anti-Virus no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] AV - Microsoft SE-FEP (EW) - SYS - {Severity2}**
  - Monitora eventos de erro e aviso específicos do Microsoft Security Essentials/Forefront Endpoint Protection no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] AV - Microsoft SE-FEP (I) - SYS - {Severity0}**
  - Monitora eventos informativos específicos do Microsoft Security Essentials/Forefront Endpoint Protection no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.

- **zz[SYS] AV - Misc AntiVirus (EW) - APP-SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de antivírus geral nos logs de eventos de aplicativos e sistemas. Os alarmes são considerados de gravidade 3.
- **zz[SYS] AV - Misc AntiVirus (I) - APP-SYS - {Severity1}**
  - Monitora eventos informativos específicos de antivírus geral nos logs de eventos de aplicativos e sistemas. Os alarmes são considerados de gravidade 1.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Symantec/Norton AntiVirus no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Symantec/Norton AntiVirus no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] AV - Symantec/Norton AntiVirus (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Symantec/Norton AntiVirus no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] AV - Symantec/Norton AntiVirus (I) - APP - {Severity0}**
  - Monitora eventos específicos informativos do Symantec/Norton AntiVirus no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.

Backup

- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso de execução de backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso de execução de backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Backup - Backup Exec (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso de execução de backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Backup - Backup Exec (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de execução de backup no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Backup - Backup Exec (EWISFCV) - APP - {Severity0}**
  - Monitora eventos específicos de execução de backup no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Backup - Backup Exec Job Failure/Cancellation (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso de cancelamento/falha de execução de backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Backup - Backup Exec Job Success (EWISFCV) - APP - {Severity0}**
  - Monitora eventos específicos de êxito de trabalho na execução de backup no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Backup - BrightStor ARCserve (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do BrightStor ARCserve no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Backup - BrightStor ARCServe (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso do BrightStor ARCServe no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Backup - Microsoft Windows Backup (E) - APP - {Severity2}**

- Monitora eventos específicos de erro de backup do Microsoft Windows no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Backup - Misc Backup (E) - APP - {Severity1}
  - Monitora eventos específicos de erro de backup geral no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Backup - Misc Backup (I) - APP - {Severity0}
  - Monitora eventos específicos informativos de backup geral no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Backup - Misc Backup (W) - APP - {Severity1}
  - Monitora eventos específicos de avisos de backup geral no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.

Banco de dados

- zz[SYS] Database - SQL Server (E) - APP - {Severity2}
  - Monitora eventos específicos de erro de SQL Server no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server (E) - APP - {Severity3}
  - Monitora eventos específicos de erro de SQL Server no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso do SQL Server - ACID no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - ACID no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - ACID (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do SQL Server - ACID no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - ACID (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de erro de SQL Server - ACID no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - Backup (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do SQL Server - backup no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - Backup (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de erro de SQL Server - backup no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso do SQL Server - recursos de banco de dados no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - recursos de banco de dados no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - DB Resources (EW) - APP - {Severity3}

- Monitora eventos específicos de erro e aviso do SQL Server - recursos de banco de dados no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - DB Resources (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de erro de SQL Server - recursos de banco de dados no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso do SQL Server - MSDTC no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - MSDTC no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - MSDTC (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do SQL Server - MSDTC no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - MSDTC (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de erro de SQL Server - MSDTC no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso do SQL Server - rede no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Database - SQL Server - Network (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - rede no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - consulta no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - Query (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do SQL Server - consulta no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso do SQL Server - replicação no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - replicação no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Database - SQL Server - Replication (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso do SQL Server - replicação no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Database - SQL Server - Replication (EWISFCV) - APP - {Severity0}
  - Monitora eventos específicos de erro de SQL Server - replicação no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity1}
  - Monitora eventos específicos de erro e aviso do SQL Server - geração de relatórios no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- zz[SYS] Database - SQL Server - Reporting (EW) - APP - {Severity2}
  - Monitora eventos específicos de erro e aviso do SQL Server - geração de relatórios no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.

- **zz[SYS] Database - SQL Server - Reporting (EWISFCV) - APP - {Severity0}**
  - ➢ Monitora eventos específicos de erro de SQL Server - geração de relatórios no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity1}**
  - ➢ Monitora eventos específicos de erro e aviso do agente SQL Server - várias instâncias no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity2}**
  - ➢ Monitora eventos específicos de erro e aviso do agente SQL Server - várias instâncias no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EW) - APP - {Severity3}**
  - ➢ Monitora eventos específicos de erro e aviso do agente SQL Server - várias instâncias no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Database - SQL Server Agent - Multiple Instances (EWISFCV) - APP - {Severity0}**
  - ➢ Monitora eventos específicos de erro do agente SQL Server - várias instâncias no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity1}**
  - ➢ Monitora eventos específicos de erro e aviso do agente SQL Server - instância única no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity2}**
  - ➢ Monitora eventos específicos de erro e aviso do agente SQL Server - instância única no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EW) - APP - {Severity3}**
  - ➢ Monitora eventos específicos de erro e aviso do agente SQL Server - instância única no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Database - SQL Server Agent - Single Instance (EWISFCV) - APP - {Severity0}**
  - ➢ Monitora eventos específicos de erro do agente SQL Server - instância única no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Database - SQL Server Cluster (I) - SYS - {Severity2}**
  - ➢ Monitora eventos específicos informativos de cluster do SQL Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Database - SQL/Service Control Manager (EW) - SYS - {Severity3}**
  - ➢ Monitora eventos específicos de erro e aviso do gerenciador de controle do SQL Server no log de eventos do sistema. Os alarmes são considerados de gravidade 3.

E-mail

- **zz[SYS] Email - Blackberry Server (E) - APP - {Severity1}**
  - ➢ Monitora eventos específicos de erro de servidor Blackberry no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity1}**
  - ➢ Monitora eventos específicos de aviso de servidor Blackberry no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Blackberry Server (W) - APP - {Severity2}**
  - ➢ Monitora eventos específicos de aviso de servidor Blackberry no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Blackberry Server Events (E) - APP - {Severity3}**

- Monitora eventos específicos de erro de eventos de servidor Blackberry no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.

- **zz[SYS] Email - Blackberry Server Events (W) - APP - {Severity2}**
  - Monitora eventos específicos de aviso de eventos de servidor Blackberry no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2000 and 2003 (E) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2000 e 2003 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2000 e 2003 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2000 and 2003 (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2000 e 2003 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2000 and 2003 and 2007 (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2000, 2003 e 2007 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 (EWISFCV) - APP - {Severity0}**
  - Monitora eventos específicos de execução do Exchange 2007 no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Acesso a cliente no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Acesso a cliente no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Client Access (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Acesso a cliente no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de borda no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de borda no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Edge Transport (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de borda no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity1}**

- Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de hub no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de hub no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Hub Transport (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Transporte de hub no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Caixa de correio no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Caixa de correio no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Caixa de correio no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 - Mailbox (EWISFCV) - APP - {Severity0}**
  - Monitora eventos específicos de execução do Exchange 2007 - Caixa de correio no log de eventos de aplicativos. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Serviços de transporte no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Serviços de transporte no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Transport Services (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Serviços de transporte no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Sistema de mensagens unificadas no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Sistema de mensagens unificadas no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange 2007 - Unified Messaging (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Exchange 2007 - Sistema de mensagens unificadas no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange 2010 Server (E) - APP - {Severity1}**
  - Monitora eventos específicos de erro de servidor Exchange 2010 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity1}**
  - Monitora eventos específicos de erro e aviso de servidor Exchange 2010 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso de servidor Exchange 2010 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.

- **zz[SYS] Email - Exchange 2010 Server (W) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso de servidor Exchange 2010 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity2}**
  - Monitora eventos específicos de erro de servidor Exchange no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Email - Exchange Server (E) - APP - {Severity3}**
  - Monitora eventos específicos de erro de servidor Exchange no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange Server (I) - SYS - {Severity3}**
  - Monitora eventos específicos informativos de servidor Exchange no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange Server 5.5 (E) - APP - {Severity3}**
  - Monitora eventos específicos de erro de servidor Exchange 5.5 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - Exchange/Service Control Manager (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso do gerenciador de controle de serviço/Exchange no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Email - SMTP/Service Control Manager (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso do gerenciador de controle de serviço/SMTP no log de eventos do sistema. Os alarmes são considerados de gravidade 3.

Hardware

- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de bateria Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de bateria Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Battery (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de bateria Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Battery (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de bateria Dell no registro de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de controlador Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de controlador Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Controller (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de controlador Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Controller (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de controlador Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.

- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de aviso e erro elétrico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de aviso e erro elétrico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Electrical (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de aviso e erro elétrico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Electrical (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos elétricos Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de carcaça Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de carcaça Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Enclosure (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de carcaça Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Enclosure (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de carcaça Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso ambientais Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso ambientais Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Environmental (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso ambientais Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Environmental (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos ambientais Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de ventoinha Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de ventoinha Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Fan (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de ventoinha Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Fan (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de ventoinha Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.

- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de alterações de hardware Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de alterações de hardware Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Hardware Changes (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de alterações de hardware Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Hardware Changes (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de alterações ambientais Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de log de hardware Dell no log de eventos de sistemas. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Hardware Log (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de log de hardware Dell no log de eventos de sistemas. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Hardware Log (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de log de hardware Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de mídia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de mídia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell Media (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de mídia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Hardware - Dell Media (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos de mídia Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso pré-falha de memória Dell no log de eventos de sistemas. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell Memory Prefailure (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso pré-falha de memória Dell no log de eventos de sistemas. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso de sistema OMSA Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso de sistema OMSA Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Hardware - Dell OMSA System (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de sistema OMSA Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.

- zz[SYS] Hardware - Dell OMSA System (EWISFCV) - SYS - {Severity0}
  - Monitora eventos específicos de sistema OMSA Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity2}
  - Monitora eventos específicos de erro e aviso de sistema OMSM Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- zz[SYS] Hardware - Dell OMSM System (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso de sistema OMSM Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity1}
  - Monitora eventos específicos de erro e aviso de disco físico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity2}
  - Monitora eventos específicos de erro e aviso de disco físico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- zz[SYS] Hardware - Dell Physical Disk (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso de disco físico Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - Dell Physical Disk (EWISFCV) - SYS - {Severity0}
  - Monitora eventos específicos de disco físico Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity1}
  - Monitora eventos específicos de erro e aviso de gestão de energia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity2}
  - Monitora eventos específicos de erro e aviso de gestão de energia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- zz[SYS] Hardware - Dell Power Management (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso de gestão de energia Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Hardware - Dell Power Management (EWISFCV) - SYS - {Severity0}
  - Monitora eventos específicos de gestão de energia Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 0.
- zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity1}
  - Monitora eventos específicos de erro e aviso de processador Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Hardware - Dell Processor (EW) - SYS - {Severity2}
  - Monitora eventos específicos de erro e aviso de processador Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- zz[SYS] Hardware - Dell Processor (EWISFCV) - SYS - {Severity0}
  - Monitora eventos específicos de processador Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity1}
  - Monitora eventos específicos de erro e aviso de espelho de redundância Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Hardware - Dell Redundancy Mirror (EW) - SYS - {Severity2}
  - Monitora eventos específicos de erro e aviso de espelho de redundância Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.

- zz[SYS] Hardware - Dell Redundancy Mirror (EWISFCV) - SYS - {Severity0}
  - Monitora eventos específicos de espelho de redundância Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity1}
  - Monitora eventos específicos de erro e aviso de temperatura Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity2}
  - Monitora eventos específicos de erro e aviso de temperatura Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- zz[SYS] Hardware - Dell Temperature (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso de temperatura Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - Dell Temperature (EWISFCV) - SYS - {Severity0}
  - Monitora eventos específicos de temperatura Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity1}
  - Monitora eventos específicos de erro e aviso de disco virtual Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Hardware - Dell Virtual Disk (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso de disco virtual Dell no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - Dell Virtual Disk (EWISFCV) - SYS - {Severity0}
  - Monitora eventos específicos de disco virtual Dell no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- zz[SYS] Hardware - HP Top Tools (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso de principais ferramentas HP no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - HP/Compaq Insight Manager (EW) - APP - {Severity3}
  - Monitora eventos específicos de erro e aviso de HP/Compaq Insight Manager no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - HP/Compaq StorageWorks (EW) - SYS - {Severity3}
  - Monitora eventos específicos de erro e aviso de HP/Compaq StorageWorks no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- zz[SYS] Hardware - IBM SeriesX Events (E) - APP - {Severity2}
  - Monitora eventos específicos de erro de eventos de IBM SeriesX no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- zz[SYS] Hardware - Misc HW (E) - SYS - {Severity1}
  - Monitora eventos específicos de erro de hardware geral no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- zz[SYS] Hardware - Misc HW (E) - SYS - {Severity2}
  - Monitora eventos específicos de erro de hardware geral no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- zz[SYS] Hardware - Misc HW (W) - SYS - {Severity1}
  - Monitora eventos específicos de aviso de hardware geral no log de eventos do sistema. Os alarmes são considerados de gravidade 1.

Infraestrutura de rede

- zz[SYS] Network Infrastructure - Active Directory (E) - SYS - {Severity1}

- Monitora eventos específicos de erro de Active Directory no log de eventos do sistema. Os alarmes são considerados de gravidade 1.

- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity1}**
  - Monitora eventos específicos de aviso de Active Directory no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - Active Directory (W) - SYS - {Severity2}**
  - Monitora eventos específicos de aviso de Active Directory no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Network Infrastructure - Active Directory Events (E) - APP - {Severity3}**
  - Monitora eventos específicos de erro de eventos de Active Directory no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Network Infrastructure - Active Directory Events (W) - APP - {Severity2}**
  - Monitora eventos específicos de aviso de eventos de Active Directory no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Network Infrastructure - Active Directory Logon/Logoff/Lockout Activity (F) - SEC - {Severity3}**
  - Monitora eventos específicos de auditoria de falha de atividade de logon/logoff/bloqueio do Active Directory no log de eventos de segurança. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erro NTDS de Active Directory no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (E) - SYS - {Severity3}**
  - Monitora eventos específicos de erro NTDS de Active Directory no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Network Infrastructure - Active Directory NTDS (I) - SYS - {Severity0}**
  - Monitora eventos específicos informativos de NTDS de Active Directory no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] Network Infrastructure - DHCP Server (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erro de servidor DHCP no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - DHCP Server (W) - SYS - {Severity1}**
  - Monitora eventos específicos de aviso de servidor DHCP no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - DNS Server (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erro de servidor DNS no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - DNS Server (W) - SYS - {Severity1}**
  - Monitora eventos específicos de aviso de servidor DNS no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Network Infrastructure - WINS Server (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erro de servidor WINS no log de eventos do sistema. Os alarmes são considerados de gravidade 1.

Acesso remoto

- **zz[SYS] Remote Access - Citrix MetaFrame (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Citrix MetaFrame no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Remote Access - Citrix Server Events (E) - APP - {Severity2}**

- Monitora eventos específicos de erro de eventos de servidor Citrix no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity2}**
  - Monitora eventos específicos de erro de eventos de servidor Terminal no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Remote Access - Terminal Server Events (E) - APP - {Severity3}**
  - Monitora eventos específicos de erro de eventos de servidor Terminal no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.

Sistemas Web

- **zz[SYS] Web Systems - IIS 6 Events (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso de eventos do IIS 6 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity2}**
  - Monitora eventos específicos de erro de eventos do IIS 7 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] Web Systems - IIS 7 Events (E) - APP - {Severity3}**
  - Monitora eventos específicos de erro de eventos do IIS 7 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] Web Systems - IIS Server (E) - APP - {Severity1}**
  - Monitora eventos específicos de erro de servidor IIS no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.
- **zz[SYS] Web Systems - IIS Server (W) - APP - {Severity1}**
  - Monitora eventos específicos de aviso de servidor IIS no log de eventos de aplicativos. Os alarmes são considerados de gravidade 1.

Plataformas de SO

- **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity2}**
  - Monitora eventos específicos de erros comuns do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server (Core) Events (E) - SYS - {Severity3}**
  - Monitora eventos específicos de erros comuns do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server (Core) Events (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos comuns do Windows Server no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity1}**
  - Monitora eventos específicos comuns de auditoria com falha do Windows Server no log de eventos de segurança. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server (Core) Events (F) - SEC - {Severity3}**
  - Monitora eventos específicos comuns de auditoria com falha do Windows Server no log de eventos de segurança. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity1}**
  - Monitora eventos específicos comuns de aviso do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server (Core) Events (W) - SYS - {Severity2}**
  - Monitora eventos específicos comuns de aviso do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server (Core) Ignore Events - (EW) - APP-SYS - {Ignore}**

- Ignora o monitoramento de eventos específicos de avisos e erros comuns do Windows Server no log de eventos de aplicativos e sistemas.
- **zz[SYS] OS - Windows Server (Core) Printer Spooler (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso de spooler de impressão do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso do gerenciador de controle de serviço do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server (Core) Service Control Manager (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso do gerenciador de controle de serviço do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server (Core) Service Control Manager (I) - SYS - {Severity2}**
  - Monitora eventos específicos informativos do gerenciador de controle de serviço do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server (Core) System Shutdown (W) - SYS - {Severity2}**
  - Monitora eventos específicos de aviso de desligamento do sistema do Windows Server no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erros comuns do Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server 2008 (Core) Events (E) - SYS - {Severity3}**
  - Monitora eventos específicos de erros comuns do Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server 2008 (Core) Events (W) - SYS - {Severity1}**
  - Monitora eventos específicos comuns de aviso do Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Advanced Windows Server 2008 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - APP - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Advanced Windows Server 2008 no log de eventos de aplicativos. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity1}**
  - Monitora eventos específicos de erro e aviso do Advanced Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Advanced Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server 2008 Advanced (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Advanced Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server 2008 Advanced (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos comuns do Advanced Windows Server 2008 no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity1}**

- Monitora eventos específicos de erro e aviso do Basic Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 1.

- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity2}**
  - Monitora eventos específicos de erro e aviso do Basic Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server 2008 Basic (EW) - SYS - {Severity3}**
  - Monitora eventos específicos de erro e aviso do Basic Windows Server 2008 no log de eventos do sistema. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Server 2008 Basic (EWISFCV) - SYS - {Severity0}**
  - Monitora eventos específicos comuns do Basic Windows Server 2008 no log de eventos do sistema. Usado somente para fins de registro em logs e geração de relatórios.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity1}**
  - Monitora eventos específicos comuns de auditoria com falha do Basic Windows Server 2008 no log de eventos de segurança. Os alarmes são considerados de gravidade 1.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity2}**
  - Monitora eventos específicos comuns de auditoria com falha do Basic Windows Server 2008 no log de eventos de segurança. Os alarmes são considerados de gravidade 2.
- **zz[SYS] OS - Windows Server 2008 Basic (F) - SEC - {Severity3}**
  - Monitora eventos específicos comuns de auditoria com falha do Basic Windows Server 2008 no log de eventos de segurança. Os alarmes são considerados de gravidade 3.
- **zz[SYS] OS - Windows Workstation (Core) Events (E) - SYS - {Severity1}**
  - Monitora eventos específicos de erros comuns de estação de trabalho com Windows no log de eventos do sistema. Os alarmes são considerados de gravidade 1.

Índice

A

B

C

D

E

F

G

H

I

M

O

P

R

S

U

V